Researchers found flaw in Apple message encryption

March 22 2016, by Ian Duncan, The Baltimore Sun

Apple issued an update to its iPhone operating system Monday that fixes a flaw identified by researchers at the Johns Hopkins University in the encryption of iMessages - the ones that show up blue when they arrive in the Messages app.

The problem is in the protocol that scrambles the messages, said Ian

Miers, one of the Hopkins researchers. Apple addressed the weakness in Monday's update, but Miers said it will likely need to develop a permanent solution.

The Hopkins team, led by Matthew D. Green, an assistant professor at the Johns Hopkins Information Security Institute, told Apple about the problems last year so the technology company would have time to develop a patch - a common practice among researchers who look for weaknesses in other people's systems.

Miers said the findings do not mean iMessage is fundamentally broken, but are a reminder of the difficulties of putting the science of cryptography into practice.

"The fact of the matter is we don't know how to do this stuff perfectly," he said.

The findings came a day before Apple's lawyers were set to face the federal government in court over a request to gain access to an iPhone that belonged to one of the attackers in the deadly San Bernardino, Calif., shooting last year.

The FBI has said data on the phone is encrypted and it needs Apple's help to get in, but the company has refused to provide aid. Late Monday, the FBI said it had a new lead on a way to get access to the phone and asked to postpone the hearing.

The case has set off a fresh battle over encryption, which is vital for carrying out private communications over the Internet. Online shopping and banking has long been encrypted, but, as the technology has become more widely implemented in popular consumer products, law enforcement has warned that it is making it increasingly difficult to gather evidence from electronic devices.

The Hopkins research doesn't have direct bearing on the San Bernardino case, but Miers, a doctoral student, said the findings show that getting encryption right is hard even under ideal circumstances and making special accommodations to help law enforcement only will make it harder.

Technical experts generally agree that it doesn't matter whether a weakness in a system is created for the benefit of a government or is the result of an oversight by computer programmers: Either way, users of the system will be less secure.

The difficulties arise in both the complicated mathematics required to scramble the message and how that's translated into software.

"Even if the pieces are correct you can assemble them wrong," Miers said. "That's what happened in this case."

To exploit the weakness, the team bombarded the intended recipient of a message with hundreds of thousands of different versions of the message, eventually revealing, piece by piece, the key to decrypt an attached photo. In theory, the weakness would apply to text-only messages too, Miers said, but the researchers weren't able to come up with a way to read them.

Apple credited the Hopkins team with finding the weakness Monday on a page describing security improvements in the new version of its iPhone operating system.

An Apple spokesman said that some of the problems had been fixed already in an earlier update of its software.

"Apple works hard to make our software more secure with every release," the company said in a statement. "We appreciate the team of

researchers that identified this bug and brought it to our attention so we could patch the vulnerability."

Bill Anderson, a cryptographer at Baltimore security company OptioLabs, said the attack doesn't sound catastrophic.

"There are always little chinks in the armor," he said.

Actually exploiting the weaknesses in iMessage probably would require the resources of a government, Miers said. For example, one would need to acquire the encrypted message in the first place.

But the findings may prompt fresh questions about whether the FBI exhausted all of its resources in the San Bernardino case before seeking Apple's help.

The company's lawyers have raised that question in court papers, and several outside experts have said they think the National Security Agency could force its way into the phone.

But FBI director James Comey recently told Congress that the government doesn't have all the capabilities people sometimes assume that it does.

"If we could have done this quietly and privately, we would have done it," he said.

Technology companies have been rolling out encryption more widely since former NSA contractor Edward Snowden leaked a cache of documents in 2013 revealing the scope of the agency's eavesdropping activities. Intelligence and law enforcement officials have complained that the disclosures caused terrorists to do more to secure their communications.

Just how widespread the disruption to U.S. intelligence gathering was remains in dispute. On Sunday, The New York Times reported that suspects behind terrorist attacks in Paris last year relied on throw-away phones to cover their tracks.

The use of so-called burners was a key plot feature in the HBO television series "The Wire," a point Snowden raised Sunday on Twitter with the show's creator David Simon.

"'The Wire' (2002) is helping the terrorists," Snowden wrote. "David Simon wanted for questioning."

The messages quickly expanded into a discussion of U.S. intelligence policy and the right to privacy.

Toward the end of the discussion, Simon tweeted, "The world is a smaller, more dangerous place with every year. Unless nationalism and religion itself is foresworn ... I want the great nations to spy their balls off and learn all they can about collective/individual intention."