Apple boosts iMessage security to fend off quantum computing attacks

February 22 2024, by Mark Gurman, Bloomberg News

Credit: Pixabay/CC0 Public Domain

Apple Inc. is upgrading the security of its iMessage app, aiming to fend off a looming future threat: advanced quantum computing attacks.

The changes will be part of a new system called PQ3, Apple said on Feb. 21. It's a more advanced type of encryption that could thwart attacks from quantum computers—still-nascent technology that can perform calculations exponentially faster than traditional machines.

The fear is that these computers could someday have the power and mathematical capabilities to break through today's tools for encrypting messages. The new security protocol has already been added to beta versions of iOS 17.4, iPadOS 17.4, macOS 17.4 and watchOS 10.4, which will roll out to all users in the coming weeks. It will replace the current security protocols for all iMessage chats by the end of the year.

Though hackers don't currently have quantum computers, they could conduct what's known as a "harvest now, decrypt later" attack. That means they steal messaging data today and then use a more advanced computer in the future to break the encryption. Apple said its new system is designed to prevent that.

The warnings about quantum computing attacks have been dire. International Business Machines Corp. executive Ana Paula Assis has said that they'll cause a "cybersecurity Armageddon." SandboxAQ Chief Executive Officer Jack Hidary said that such computers will be available by the end of the decade and cause a "train wreck" for security. Governments are also getting involved, with the U.S. Senate passing a bill two years ago to address the threat.

Apple said that PQ3 "has the strongest security properties of any at-scale messaging protocol in the world." The company sees the defenses as more powerful than those of messaging app Signal, which has long been known as the gold standard for encrypted communications.

Apple considers its new system to be at a Level 3 of security, while it puts Signal at Level 2. The prior protocol for iMessage ranked as a Level

1, in Apple's view, the same level as Meta Platforms Inc.'s WhatsApp. Other popular messaging apps—like Telegram, Skype, QQ and WeChat—sit below that, according to Apple's analysis of messaging app security.

The company also said its current Contact Key Verification system, which allows users to verify that they're actually communicating with the intended person, is coming to its Vision Pro headset. The change will be included with the visionOS 1.1 software update. Users with the feature enabled on their Apple devices previously had to disable it to send messages on the Vision Pro.

Citation: Apple boosts iMessage security to fend off quantum computing attacks (2024, February 22) retrieved 10 May 2024 from https://techxplore.com/news/2024-02-apple-boosts-imessage-fend-quantum.html