Apple is already defending iMessage against tomorrow's quantum computing attacks

Apple's security team claims to have achieved a breakthrough "that advances the state of the art of end-to-end messaging." With the upcoming release of iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4, the company is bringing a new cryptographic protocol called PQ3 to iMessage that it purports to offer even more robust encryption and defenses against sophisticated quantum computing attacks.

Such attacks aren't yet a broad threat today, but Apple is preparing for a future where bad actors try to unwind current encryption standards and iMessage's security layers with the help of massively powerful computers. Such scenarios could start playing out by the end of the decade, but experts agree that the tech industry need to start defending against them well in advance.

"PQ3 is the first messaging protocol to reach what we call Level 3 security — providing protocol protections that surpass those in all other widely deployed messaging apps," the security team wrote. Yes, Apple came up with its own ranking system for messaging service security, and iMessage now stands alone at the top thanks to these latest PQ3 advancements.

In the company's view, they're enough to put Apple's service above Signal, which itself recently rolled out more sophisticated security defenses. (For reference, the current version of iMessage ranks as level 1 alongside WhatsApp, Viber, Line, and the older version of Signal.) "More than simply replacing an existing algorithm with a new one, we

rebuilt the iMessage cryptographic protocol from the ground up to advance the state of the art in end-to-end encryption," Apple wrote.

Apple says that hackers can stow away any encrypted data they obtain today in hopes of being able to break through in several years once quantum computers become a realistic attack vector:

> *Although quantum computers with this capability don't exist yet, extremely well-resourced attackers can already prepare for their possible arrival by taking advantage of the steep decrease in modern data storage costs. The premise is simple: such attackers can collect large amounts of today's encrypted data and file it all away for future reference. Even though they can't decrypt any of this data today, they can retain it until they acquire a quantum computer that can decrypt it in the future, an attack scenario known as Harvest Now, Decrypt Later.*

You can read all the nitty-gritty details on PQ3 in Apple's blog post, which is a great example of the company's focus on protecting user data. And as we've learned in recent months, Apple won't hesitate to shut out third parties – even those with well-meaning intentions – that attempt to encroach on its iPhone-selling messaging platform in any way.

https://www.theverge.com/2024/2/21/24079081/apple-imessage-pq3-post-quantum-cryptography