Google announces new algorithm that makes FIDO encryption safe from quantum computers

Getty Images

reader comments

41 with

The FIDO2 industry standard adopted five years ago provides the most secure known way to log in to websites because it doesn’t rely on passwords and has the most secure form of built-in two-factor authentication. Like many existing security schemes today, though, FIDO faces an ominous if distant threat from quantum computing, which one day will cause the currently rock-solid cryptography the standard uses to completely crumble.

Over the past decade, mathematicians and engineers have scrambled to head off this cryptopocalypse with the advent of PQC—short for post-quantum cryptography—a class of encryption that uses algorithms resistant to quantum-computing attacks. This week, researchers from Google announced the release of the first implementation of quantum-resistant encryption for use in the type of security keys that are the basic building blocks of FIDO2.

The best known implementation of FIDO2 is the passwordless form of authentication: passkeys. So far, there are no known ways passkeys can be defeated in credential phishing attacks.

Dozens of sites and services now allow users to log in using passkeys, which use cryptographic keys stored in security keys, smartphones, and other devices.

“While quantum attacks are still in the distant future, deploying cryptography at Internet scale is a massive undertaking which is why doing it as early as possible is vital,” Elie Bursztein and Fabian Kaczmarczyck, cybersecurity and AI research director, and software engineer, respectively, at Google wrote. “In particular, for security keys this process is expected to be gradual as users will have to acquire new ones once FIDO has standardized post-quantum cryptography resilient cryptography and this new standard is supported by major browser vendors.”

The path to PQC is fraught with risks. RSA and other encryption algorithms have been in use for decades with no known ways for them to be broken. Over the years, that track record has led to confidence that they are safe for use. PQC algorithms are in their infancy, and that has rightly led to concern that they can’t yet be trusted. A case in point: a PQC algorithm called SIKE. Last year, after advancing as a fourth-round candidate in a program run by the US Department of Commerce’s National Institute of Standards and Technology, SIKE was completely and spectacularly broken by a single classical computer.

The PQC algorithm used in the implementation of FIDO2 security keys takes a more cautious approach. It combines the elliptic curve digital signature algorithm—believed to be unbreakable by classical computing but easily broken with quantum computing—with a PQC algorithm known as Crystals-Dilithium. Crystals-Dilithium is now one of three PQC algorithms selected by NIST for use with digital signatures.

Advertisement

The particular Dilithium used in the recently released digital key implementation appears to solve a variety of problems.

First, for it to be broken, an attacker would have to defeat both the ECDSA encryption and the PCQ encryption that underpins its security. And second, the keys it uses are tiny compared to many other PQC algorithms in circulation now. In this week's post, the Google researchers wrote:

> *Our proposed implementation relies on a hybrid approach that combines the battle tested ECDSA signature algorithm and the recently standardized quantum resistant signature algorithm, Dilithium. In collaboration with ETH, we developed this novel hybrid signature schema that offers the best of both worlds. Relying on a hybrid signature is critical as the security of Dilithium and other recently standardized quantum resistant algorithms haven't yet stood the test of time and recent attacks on Rainbow (another quantum resilient algorithm) demonstrate the need for caution. This cautiousness is particularly warranted for security keys as most can't be upgraded — although we are working toward it for OpenSK. The hybrid approach is also used in other post-quantum efforts like Chrome's support for TLS.*
>
> *On the technical side, a large challenge was to create a Dilithium implementation small enough to run on security keys' constrained hardware. Through careful optimization, we were able to develop a Rust memory optimized implementation that only required 20 KB of memory, which was sufficiently small enough. We also spent time ensuring that our implementation signature speed was well within the expected security keys specification. That said, we believe improving signature speed further by leveraging hardware acceleration would allow for keys to be more responsive.*
>
> *Moving forward, we are hoping to see this implementation (or a variant of it), being standardized as part of the FIDO2 key specification and supported by major web browsers so that users' credentials can be protected against quantum attacks. If you are interested in testing this algorithm or contributing to security key research, head to our open*

source implementation OpenSK.

The security of RSA and other traditional forms of asymmetric encryption is based on mathematical problems that are easy to verify the answer to but hard to calculate. RSA, for instance, relies on the difficulty of factorizing prime numbers. Finding the primes for the number 27,919,645,564,169,759 is hard, but once someone is told the primes are 48,554,491 and 575,016,749 it takes a few seconds to verify (thanks to Boot.dev for the example).

Advertisement

A factorization method known as Shor's algorithm makes it theoretically possible to solve these types of problems. That, in turn, means certain death for many of the cryptographic schemes now protecting encrypted web sessions, banking and medical data, and other secrets. The only thing holding back this doomsday scenario is the massive amount of quantum computing resources required.

While classical computers can't run Shor's algorithm efficiently enough to break RSA keys in use today, quantum computers with sufficient power will be able to solve them in a matter of eight hours. No one knows when that day will come, though one expert in the field said recently it won't be in our lifetime. Still, as the Google researchers pointed out, adopting any PQC schemes will be slow, so it makes sense to begin work sooner rather than later. https://arstechnica.com/?p=1961906