Cryptography

Quantum cyberattacks: Preparing your organization for the unknown

March 17, 2021 by **Rodika Tollefson**

Quantum computing days are coming

Quantum computing has been a buzzword for several years. And while it's still the early days, several industries have been showing progress, and 2020 brought a slate of new developments. As the technology inches closer to real-world applications, some leading companies are preparing for another future reality: quantum cyberattacks.

What are quantum cyberattacks?

A quantum cyberattack means a sophisticated attack that uses quantum computing to do things like break the strongest encryption or quickly analyze massive amounts of data sets to infect a large number of networks with malware.

In this Series

Quantum computers, while still in development, rely on the principles of quantum physics to tackle computational problems that classical computers can't. Traditional computers represent data in the binary values of either 1 or 0. Quantum computing uses qubits (quantum bits), which could superimpose the ones and the zeros — in other words, store or represent the bits simultaneously.

In cryptography, as an example, the popular public-key cryptosystem RSA's algorithms rely on prime factorization to achieve asymmetric encryption using key sizes of 1,024 bits. The secret key is a set of large prime numbers, and factoring prime numbers would be extremely time-consuming for classical computing systems. It would take even the fastest supercomputers thousands of years to solve that type of complex problem.

A quantum computer, on the other hand, could solve the factoring problem millions of times faster — enabling the quick extraction of the decryption key without the need for brute force. Some researchers estimate that it would likely take a computer with 250 million qubits to crack modern encryption algorithms.

Other types of algorithms could be defeated with brute force, using quantum computing to significantly accelerate the process. To prevent this from happening, the size of the key would need to be increased — but it could take the industry a decade or longer to phase out pre-quantum algorithms.

Introduction to Public Key

How much of a reality are quantum cyberattacks?

Although quantum computing dates back to the 1980s and even earlier, the industry itself is just emerging. A robust quantum computer is probably still a decade away. Even so, research firm Markets and Markets estimates the quantum computing market to grow from $93 million in 2019 to $283 million by 2024 — a nearly 25% annual compound growth rate.

Many companies have been pioneering quantum computing applications in different industries, ranging from retail logistics and finance to insurance and automotive. Google, IBM, Honeywell and D-Wave are among the top players in the space. IBM, for example, made a 65-qubit computing system available in 2020 in the cloud, with plans for a 127-qubit system to be released in 2021 and 433-qubit in 2022.

Given these early developments, quantum cyberattacks are still a distant reality. But sophisticated threat actors such as nation-states have already been investing in quantum technology research and development — and experts believe it's only a matter of time before they use it to try to hack systems such as encrypted communications.

The race to prevent quantum computing attacks

Cryptographers and other cybersecurity experts aren't waiting for the days when quantum computing becomes widespread. Researchers from around the world, including from academia, government and companies like Visa Inc. and JPMorgan, have been studying post-quantum cryptography for several years in anticipation of the future need to withstand quantum cyberattacks.

The National Institute of Standards and Technology (NIST) is also leading a post-quantum cryptography project, examining proposals for standardizing quantum-resistant public-key cryptographic algorithms. As of mid-2020, NIST had gone through three rounds of selecting candidate algorithms for the standardization and has narrowed the list to seven from the initial 69.

According to NIST, "Some engineers predict that within the next 20 or so years, sufficiently large quantum computers will be built to break essentially all public-key schemes currently in use." But, NIST notes, the need to act is now because historically it's taken more than two decades to implement the infrastructure for public-key cryptography.

What should your organization prepare for?

As mathematician Lily Chen, leader at NIST and the Technology's Cryptographic Technology Group, put it, "For public-key cryptography, the damage from quantum computers will be catastrophic." Before that happens, organizations need to start looking at stronger cryptography methods — and that means now, security experts say.

While developing these methods requires big cybersecurity budgets, experts say that even smaller companies can play a role by encouraging their large technology vendors to pursue quantum-safe encryption methods. In the meantime, organizations can also start taking steps to get the IT infrastructure ready for quantum computing.

Paul Lucier of ISARA, which specializes in "crypto-agile and quantum-safe security solutions," writes in the ISACA blog, "When it comes to quantum preparedness, a good first step is for organizations to inventory their systems and locate and identify where their cryptography is deployed."

He recommends the following steps for businesses:

- Research and understand how quantum computing will impact public-key cryptography in your company.
- Catalog where and how cryptography is used in your company.
- Prioritize the high-value assets that you'll need to migrate.
- Create a migration strategy with your team.
- Look for outside partners and tools who can help with the process.

What's next?

It's a good idea for organizations to follow NIST's developments since the standardization project will lay the foundation for making infrastructures quantum-secure. Once NIST chooses a finalist for new encryption standards, your organization should consider deploying a hybrid infrastructure as an intermediary step, coupling existing solutions with a post-quantum method. But you should start planning now — like any infrastructure migration project, preparing for the age of quantum cyberattacks will take time.

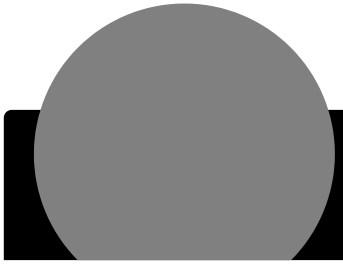
Sources

- "What is RSA Cryptography? Complete Guide to this Encryption Algorithm," Blockonomi
- "Quantum Computing: Threat to Cybersecurity?"CISO Mag
- Quantum Computing Market, Markets and Markets
- "6 experts share quantum computing predictions for 2021," TechRepublic
- "The quantum computing race the US can't afford to lose," The Next Web
- Post-Quantum Cryptography Project, NIST
- "Implications of Quantum Computing for Encryption Policy," Carnegie Endowment for International Peace

- "Quantum Hacking Could Be 'Catastrophic' If We Don't Develop Better Cryptography," Gizmodo
- "Six Steps to Start Readying for Quantum," ISACA blog

Posted: March 17, 2021

Share:



Articles Author

Rodika Tollefson

VIEW PROFILE

Rodika Tollefson splits her time between journalism and content strategy and creation for brands. She's covered just about every industry over a two-decade career but is mostly interested in technology, cybersecurity and B2B topics. Tollefson has won various awards for her journalism and multimedia work. Her non-bylined content appears regularly on several top global brands' blogs and other digital platforms. She can be reached at seattletechnologywriter.com.