accenture

A WORLD WITHOUT ENCRYPTION: QUANTUM THREATS TO CYBERSECURITY

VIDEO TRANSCRIPT

Encryption is woven into the very fabric of our lives. It establishes trust and safeguards our secrets. While you might not think about encryption as you move through your day, it's nearly always there. Every time you send an email or a text message, pay a bill from your bank account, buy groceries with your credit card, or scan your boarding pass at the airport or a ticket at a concert or sporting event, encryption is at work. Beyond these examples, encryption is working even deeper in the background, doing things like keeping your health care records safe and allowing your doctor to quickly receive new test results and share them with specialists.

The technology enabling this security dates back to the 1970s and is effective because of the difficulty of certain math problems, such as factoring large numbers. For example, while the factors of 15 are three and five, factoring larger numbers becomes significantly more challenging. This simple concept safeguards the most common cryptography used today: RSA encryption. This encryption algorithm is quite technical and is not itself a factoring algorithm, but if the publicly available input to the algorithm could be factored, then the encryption is broken. In practice, RSA uses numbers that can be more than 600 digits long, which could take current computers thousands of lifetimes to factor. Because of that, our online communication and digital identities are secure today and were thought to be secure forever.

However, all this will change in the era of quantum computing. Unlike our everyday computers, quantum computer hardware fundamentally relies on certain properties of nature at the atomic and subatomic levels. This gives quantum computers the potential to push technological boundaries and solve some of the most complex problems, such as drug discovery, medical imaging, materials science, and more. But it also poses a threat to our current encryption methods. The next generation of quantum computers will be able to quickly break RSA encryption by factoring the publicly available number used in the algorithm. The cryptographic foundation we've trusted for decades now has an expiration date. And that's not just for data sent from one place to another. It's also for vast databases of stored information which could be copied and held until a quantum computer that is powerful enough to decrypt it is developed. These are sometimes called a steal now decrypt later or SNDL attack.

But it's not all bad news. New quantum-resistant cryptographic algorithms are being developed. In 2017, for example, the National Institute of Standards and Technology, or NIST, launched a competition to develop post-quantum cryptography or PQC algorithms.

The competition is in its final stages, and governments and organizations worldwide are sending a clear signal: Now is the time to pay attention to the effect that quantum computing will have on the world. That's why leading organizations around the globe are coming together to design a Quantum Security Maturity Index that tracks five key steps to preserve the safety and security the world relies on.

Step one: Strategy. Your organization must first understand the challenges of quantum computing and educate stakeholders. This includes creating a quantum risk analysis and developing a multiyear plan towards quantum safety.

Step two: Discovery. Evaluate your organization's current cryptographic posture. Inventory all crypto-enabled products and services inside your organization and within its ecosystem, and process the risk quantum computing poses to each. Then establish requirements for partners and providers.

Step three: Architecture. Select a quantum-safe architecture, which could range from the direct replacement of current approaches for PQC to a more crypto-agile program to modernize the entire cryptographic suite. Then test components for interoperability, performance, security, and availability.

Step four: Deployment. Based on test environment trials, evolve your overall architecture and begin your enterprise rollout program, and soon after your ecosystem interoperability program.

And step five: Operations. At this point, managing your quantum-safe infrastructure will become your steady state. New threats will be seamlessly resisted by your architecture.

New technologies will be incorporated into your infrastructure, and exceptions will be quickly processed. In the face of quantum computing's advancements, our collective effort today will determine a secure and resilient digital future for generations to come. It will take years for the world's enterprises to update their old vulnerable encryption. And that's why it's imperative that we work collectively and with urgency. The time to start preparing is now!