Electronic Design

ALAN GRAU, VP of IoT/Embedded Solutions, Sectigo, https://sectigo.com/

How to Protect Your Digital Systems from the Quantum Apocalypse

Don't let the potentially cataclysmic quantum-computing onslaught catch you and your systems off-guard. Take these steps to upgrade to a quantum-safe PKI security infrastructure and move to automated certificate management.

The Quantum Apocalypse is coming. Sound scary? Well, it can be. While there's much upside to the development of quantum computing, it also brings an incredible and potentially crippling risk to our digital systems. The National Institute for Standards and Technologies (NIST), big tech companies like IBM and Google, governments, and prominent programmers all contribute to the protocols and infrastructure advancement required for quantum computing.

Quantum computing represents much more than faster processing. While it's true that quantum computers will process massive volumes of data at extraordinary speeds, the real breakthrough is that they utilize a fundamentally different approach to computing. This approach allows quantum computers to solve certain types of problems that currently take thousands of years in just seconds.

Two of the problems that quantum computers will solve very quickly is breaking the underlying math problems that make Rivest–Shamir–Adleman (RSA) and elliptic-curve-cryptography (ECC) encryption algorithms secure. Public-key-infrastructure (PKI) systems are based on these encryption algorithms.

Quantum computing is already here, albeit at an experimental stage. These systems are rapidly advancing, and it's estimated that they will begin rendering the world's current cryptographic underpinnings obsolete in the next five to 10 years.

Quantum Computers Spell the End for Today's Public-Key Cryptography

At some stage during their development, quantum computers will be fast enough to break our current ECC and RSA encryption algorithms. These algorithms are the bedrock of the PKI systems we use to authenticate and protect the identity of almost every user, system, and device. Typically, anytime you use a digital certificate you have an RSA and ECC encryption, which are very secure today.

However, soon, attacks with a sophisticated quantum computer will be very efficient at solving specific problems, such as factoring prime numbers, which underpin what makes RSA encryption secure. Quantum computing will be able to easily break those encryption algorithms in seconds and render layers of security obsolete. This inevitable day could be so crippling to society that the security sector has deemed it the "Quantum Cryptographic Apocalypse."

The hype isn't unfounded. RSA and ECC algorithms are used to secure every data source and system across industries: factories, data farms, utilities, eCommerce, banking systems, transportation, communication networks, and much more.

Right now, the dark side of quantum computing is speculative and realized chiefly by well-funded bad actors and rogue nation-states. But, like all technology, over time, quantum computing will become more accessible and mainstream. It's critical that your organization is prepared for the day when quantum computing becomes usable and affordable on a widespread scale.

If you think your data, devices, and systems are safe until doomsday, think again. Many bad actors are preparing for the looming Quantum Apocalypse by recording personal or sensitive information from credit-card transactions and medical information to access cards and ID badges that they know they can compromise in the near future.

It's important to note that not all encryption algorithms are rendered insecure by quantum-computing attacks. AES (Advanced Encryption Standard) encryption, for example,

Follow these six steps when migrating to quantum-safe cryptography.

is secure against quantum-computing attacks. AES encryption, while still an important part of security solutions, isn't an asymmetric encryption algorithm and can't be used to implement PKI solutions.

Plan Survival with Quantum Cryptography

Fortunately, researchers are getting ahead of this imminent threat.

NIST is in the process of creating new encryption algorithms based on different mathematical techniques that can be performed on traditional computers but aren't easily broken by quantum computers. They identified a number of candidate algorithms to resist quantum-computer attacks and expect to announce the first set of standard algorithms as soon as 2022.

Migrating to quantum-safe crypto algorithms requires deliberate planning and sufficient time to update systems. There's an urgency around this problem and pressing warnings by security professions to start planning now. The Quantum Apocalypse can emerge as soon as 2026, and it will take at least that long to update your systems and devices.

The number of systems and solutions using traditional encryption algorithms is vast: every website, machine, internal data management, and communications system, as well as every third-party application, server, and system, will need to be updated. Even IoT devices being built today need to have a path for new encryption over time.

Survival planning isn't just for "the other guy." There are steps you can take now to prepare your environment.

Adopt a Direct or Hybrid Migration Plan Now

For large enterprises, these measures will be a significant undertaking. A direct "rip-and-replace" approach to upgrading their encryption systems simply isn't viable for many companies. Fortunately, all systems needn't be updated simultaneously. Preparation can involve a gradual and low-risk migration of systems to these new crypto algorithms to avoid having to update and test all systems at once.

Organizations can utilize hybrid certificates to undertake a gradual yet safe migration. Hybrid certificates are X.509 certificates with both traditional RSA or ECC keys and new quantum-safe keys. Hybrid certificates enable devices that don't yet support quantum-safe crypto to work with new systems that do support quantum-safe crypto, thereby supporting a gradual migration of critical systems to quantum-safe crypto.

To complete the migration, once all systems are upgraded to support quantum-safe crypto, the hybrid certificates can be dropped in favor of pure quantum-safe certificates. However, there are multiple paths to consider for this evolution.

Some organizations may choose to move directly from traditional crypto to quantum-safe crypto *without* the hybrid certificate transition period. For industrial and enterprise environments where all systems can be simultaneously upgraded to pure quantum-safe certificates, it's possible to bypass the transition period with hybrid certs. However, this quicker, direct migration introduces much more risk. If any system isn't updated correctly, it will no longer be able to communicate with other systems.

Six Steps for Migrating to Quantum-Safe Cryptography

It's vital that you're informed and ready to migrate to new cryptographic standards as soon as they're available. There are six steps to successfully migrate to quantum-safe cryptography—whether upgrading directly or using hybrid certificates *(see figure)*.

Step 1: Upgrade to a quantum-safe PKI security infrastructure.

The first step toward migrating to quantum-safe cryptography is to upgrade the PKI, including the certificate authority (CA), to utilize quantum-safe crypto algorithms. Whether using an in-house PKI system or adapting a solution from a publicly trusted CA, it's critical that the CA provide support for quantum-safe crypto algorithms and quantum-safe certificate issuance. If your IT security team chooses to use hybrid certificates, they must select a CA that supports both hybrid certificates and pure quantum-safe certificates.

Step 2: Update server applications to recognize and use new crypto algorithms.

Migrating to quantum-safe crypto requires updating the crypto libraries used by server applications to support both the new crypto algorithms and the new quantum-safe certificate formats. If hybrid certificates are used, server applications will need to recognize and process both traditional RSA/ECC certs and hybrid certs containing quantum-safe crypto keys. This requires the server applications to distinguish between the two different certificate types and handle each with the proper crypto algorithm for that certificate

type.

Step 3: Update client crypto algorithms.

Next, IT and development teams will need to update a wide range of client applications to use quantum-safe crypto algorithms. Once fully and safely upgraded, administrators can discontinue the use of traditional RSA/ECC keys/certificates in client applications and instead use the new quantum-safe equivalents.

The exception to this step is when a client application communicates with multiple server applications that may not all be simultaneously upgraded to quantum-safe crypto. In this case, hybrid certificates will allow the client to work with servers supporting traditional RSA/ECC crypto, while at the same time, use quantum-safe algorithms with servers that support these newer algorithms.

Step 4: Install quantum-safe roots on all systems.

Each system utilizing PKI has a trusted root store. This root store contains the certificates for the root and intermediate CAs that issue certificates within the PKI system. Once systems are updated to support quantum-safe crypto algorithms, these root stores must also be updated to add the new root and intermediate certificates.

Step 5: Issue new quantum-safe certificates to connected devices and applications.

After your company's systems are updated to support quantum-safe crypto, the next step is to issue new certificates and install them on all endpoints. Once completed, each device can begin using quantum-safe crypto algorithms, as enabled by the new certificates.

Step 6: Get rid of the old.

The final step in migrating to quantum-safe crypto is to deprecate the traditional encryption algorithms so that they're no longer used. This can be done gradually as applications and systems are migrated to the new algorithms. After all systems are migrated, the root ECC and RSA certificates should be revoked, ensuring they're not used by any systems.

Protect Your Quantum Future

The time to take the first step of upgrading to a quantum-safe PKI security infrastructure and moving to automated certificate management is now. Migrating to new crypto algorithms and PKI systems requires issuing large numbers of new certificates as each device/application will require a new certificate.

Today, easy-to-use certificate management platforms enable automated certificate discovery and renewal to ensure systems don't fail due to an expired certificate and ease the administrative burden of installing new certificates on devices and systems. Support for automation tools should be a top priority for security teams considering a new PKI solution.

Yes, quantum computers are large, complex, and expensive systems that, at first, will only be affordable for major international technology organizations. However, their use could then spread to various nation-states, and eventually to cybercriminals and hackers.

The good news is that by being informed and taking certificate migration steps, you can alleviate risks and reduce vulnerability to attacks using quantum computers.

Alan Grau has 30 years of experience in telecommunications and the embedded software marketplace. He is VP of IoT/Embedded Solutions at Sectigo, the world's largest commercial Certificate Authority and a leading cybersecurity provider of digital identity solutions. Alan joined Sectigo in May 2019 as part of the company's acquisition of Icon Labs, a provider of security software for IoT and embedded devices, where he was CTO and co-founder. He's a frequent industry speaker and blogger and holds multiple patents related to telecommunication and security. Prior to founding Icon Labs, Alan worked for AT&T Bell Labs and Motorola. He has an MS in computer science from Northwestern University.