The Search for Quantum-Resistant Cryptography: Understanding the Future Landscape

Submitted by: Sectigo
Monday, 30 September 2019

Sectigo Announces a Broad Set of Resources to Educate the Cybersecurity Community About the Implications of Quantum Computing on PKI

ROSELAND, N.J. – September 30, 2019 – Quantum computing is set to transform the IT industry. This new computing architecture takes advantage of quantum mechanics to deliver capabilities beyond what traditional binary computing can achieve. However, these capabilities come at a cost. Once quantum computers reach a certain state of maturity, they are destined to render the cryptographic underpinnings of today's digital systems insecure.

To help enterprises prepare for the implications of quantum computing, Sectigo (https://sectigo.com/), the world's largest commercial Certificate Authority (CA) and a provider of purpose-built and automated PKI management solutions, has created a broad set of 15 educational resources for security industry professionals in the form of a whitepaper, podcast episodes and transcriptions, and articles.

By its nature, quantum computing (https://whatis.techtarget.com/definition/quantum-computing) is highly effective at factorizing numbers, which means quantum computers will be many orders of magnitude faster at the calculations necessary to break the RSA and ECC (Elliptic Curve Cryptography) encryption that underpins our digital systems today. This efficiency gain is so monumental that increasing the key sizes of these cryptographic schemes is not a viable solution. Rather, the world's Public Key Infrastructure (PKI) systems will have to migrate to one or more new, quantum-resistant encryption algorithms before quantum computers break current encryption methods.

PKI is necessary for the secure operation of all the confidential and mission-critical digital processes in our global economy, including finance, commerce, communication, enterprise computing, transportation, defense, manufacturing, healthcare, government, and logistics. The impact of insecure PKI would be so vast that this potential outcome has come to be known as the Quantum Apocalypse.

The Search for Algorithms is Underway

Thought leaders from industry, academia, and government are combining efforts to discover and deploy quantum-resistant cryptographic solutions across our global digital systems. The National Institute for Standards and Technology (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography) (NIST) has been leading an effort to identify one or more cryptographic approaches that can substitute for RSA and ECC. The community participating in NIST's process now has a list of more than 20 candidate algorithms (https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions) that are undergoing scrutiny of their suitability for this task.

Successful quantum-resistant algorithms must be difficult to break using brute-force attacks by both traditional and quantum architectures while still meeting performance standards similar to today's algorithms. To be viable for widespread use, the algorithm must deliver on criteria such as:

Fast encryption using traditional computers
Fast decryption (with private keys) using traditional computers
Impractical to decrypt (without private keys) using quantum or traditional computing architectures
Able to generate encrypted data of a size that is reasonable for storage and transmission across networks and the internet
Compatible with a vast range of software, hardware, and services
Well-understood and checked against potential attacks

Understanding the Challenge – Available Resources

“While no one can definitively say when quantum computers will reach the point of defeating RSA and ECC, many estimates place that date in the next 10 or 15 years. Any organization that does not migrate by then will be vulnerable,” said Tim Callan, Senior Fellow, Sectigo. “At Sectigo, we are working with our large base of enterprises, schools, and government agencies to help them achieve crypto agility by putting in place the systems and automation capabilities necessary to ensure rapid and comprehensive migration to these new standards once they arrive.”

To educate the cybersecurity community, Sectigo has the following quantum-resistant cryptography resources available:

Whitepaper

The Search for Quantum Resistant Cryptography
(https://sectigo.com/resources/the-search-for-quantum-resistant-cryptography)

Root Causes Podcast Episodes & Blog Posts:

Cryptographic Quantum Apocalypse (Transcript) (https://sectigo.com/resources/root-causes-1-05)
Quantum-Resistant Cryptography (Transcript) (https://sectigo.com/resources/root-causes-1-06)
Mosca's Inequality, Mad Max, and Mohawks (Transcript) (https://sectigo.com/resources/root-causes-1-35)
The Search for Quantum-Resistant Crypto (Transcript) (https://sectigo.com/resources/root-causes-1-36)
Will Quantum Annealing Break Cryptography? (https://sectigo.com/resources/root-causes-1-37)
Entropy and Random Numbers (Transcript)
(https://soundcloud.com/tim-callan/root-causes-1-25-entropy-and-random-numbers)

Articles

Forbes: Quantum-Resistant Cryptography: Our Best Defense Against an Impending Quantum Apocalypse
(https://www.forbes.com/sites/forbestechcouncil/2019/09/25/quantum-resistant-cryptography-our-best-defense-against-an-imp

Datacenter Dynamics: Cryptographic Security and the Quantum Apocalypse
(https://www.datacenterdynamics.com/opinions/cryptographic-security-and-quantum-apocalypse/)

About Sectigo

Sectigo provides award-winning (https://sectigo.com/awards) purpose-built and automated PKI management solutions to secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority, trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit www.sectigo.com (https://sectigo.com/).
###

Elliot Harrison
Positive
+44 (0)20 3637 0649
eharrison@positivemarketing.com

Ines Mitsou
Positive
+44 (0)20 3637 0640
imitsou@positivemarketing.com