Wednesday, August 20, 2025

12:10 PM - 12:30 PM

Navigating the Quantum Era: A Proactive Approach to Post-Quantum Cryptography

Phil Brown

Chief Architect, Army, Defense Agencies, and Special Operations Forces

Cisco

Abstract:

Cisco is actively engaged in developing and implementing post-quantum cryptography (PQC) to secure its networks, applications, and data against the emerging threat posed by quantum computing which could act as a “game-changer” for assured voice and data communications at echelon to secure data. The company's comprehensive strategy focuses on a seamless and proactive transition from classical cryptographic methods to quantum-resistant algorithms, emphasizing the protection of boot integrity, control plane integrity, and data plane integrity across its infrastructure. Cisco collaborates closely with leading organizations such as the National Institute of Standards and Technology (NIST) and the Internet Engineering Task Force (IETF) to validate and integrate standardized PQC algorithms into its solutions, ensuring interoperability and robust security. Rather than an immediate overhaul, Cisco advocates for a phased, incremental deployment approach, integrating hybrid cryptographic models that combine classical and quantum-safe techniques during the transition period. This includes evaluating the impact of PQC on both existing and future networking hardware, ensuring that its routers, switches, and security appliances can seamlessly support new cryptographic primitives. Furthermore, Cisco is developing quantum-resistant software products, including crypto software libraries that support NIST's PQC algorithms and protocol standards.

Cisco has been actively developing and deploying post-quantum trust anchors designed to resist attacks from large-scale quantum computers, with new quantum-safe editions of Secure Boot and Cisco Trust Anchor Technologies, implementing the new NIST PQC standards, anticipated soon. Notably, some existing products, such as the Cisco 8100 router, Cisco Catalyst 9500 network switch, and Cisco Firewall 4215, already provide quantum-safe secure boot using hash-based signatures (HBS), a precursor to the NIST-approved LMS, with Cisco PQC hardware based on the new NIST standards expected to be available in late 2025 or 2026.

Beyond hardware and software, Cisco is evolving its cloud-native security solutions and Zero Trust architectures to incorporate quantum-resistant authentication and encryption, aiming to protect sensitive data in transit and at rest. The company is also a founding member of the Linux Foundation's Post-Quantum Cryptography Alliance, including the Open Quantum Safe (OQS) project, to facilitate agreement on standards implementation and smooth the transition. To accommodate new algorithms, Cisco is working on incorporating PQC algorithms into transport protocols like TLS, SSH, and IKEv2, in parallel with IETF's efforts to release key standards.