Quantum Computing Puts Cybersecurity at Risk

Posted by Okachinepa 11/14/2024

Courtesy of SynEvol
Credit: National Center for Supercomputing Application

Similar to artificial intelligence, quantum computing is developing quickly in the field of high-performance computing. What will happen, though, if this potent new technology surpasses the security and cyberinfrastructure we currently depend on?

Researchers at the National Center for Supercomputing Applications are working proactively to address this challenge before it becomes a pressing issue.

According to NCSA Research Scientist Phuong Cao, "the problem is urgent because in the next ten years, practical quantum computers will break classical encryption." Adopting post-quantum cryptography (PQC) or quantum-resistant cryptographic network protocols is a crucial step toward democratizing quantum computing. It is still unclear how post-quantum cryptography will be supported by current cyberinfrastructure.

At the IEEE International Conference on Quantum Computing and Engineering in Montreal in September, Cao and Jakub Sowa, an undergraduate student at the University of Illinois Urbana-Champaign who is a member of the CyberCorps: Scholarship for Service and the Illinois Cyber Security Scholars Program, presented a paper on this subject. They presented the latest findings on the adoption rate of PQC across a wide range of network protocols, described the current state of PQC implementation in important scientific applications such as OpenSSH and SciTokens, emphasized the difficulties of being quantum-resistant, and emphasized the discussion of potential novel attacks. Their findings also suggested the design of a novel PQC network instrument housed at NCSA and the University of Illinois and integrated as part of the FABRIC testbed.

According to Cao, "the main challenges of adopting PQC lie in hardware, software, and network implementation as well as algorithmic complexity." "Our results demonstrate that only OpenSSH and Google Chrome have successfully implemented PQC and achieved an initial adoption rate of 0.029% at this time. This is the first large-scale measurement of PQC adoption at national-scale supercomputing centers."

The U.S. National Science Foundation (NSF) has awarded Cao $200,000 as the primary investigator for a project titled "Quantum-Resistant Cryptography in Supercomputing Scientific Applications." Universities and research facilities will be able to transition to PQC in order to protect sensitive data and scientific research, and a network instrument will be able to assess the adoption rate of PQC. By showcasing the growing adoption rate over time, the initiative will establish public confidence in the security of scientific computing and serve as a national model for transforming cyberinfrastructure to be quantum resistant.

"It will take a long time to switch to PQC algorithms across sectors," Nikolich stated. "The first step in comprehending the extent of the issue among the scientific infrastructure community will be our effort. We will have good visibility into the situation because FABRIC operates in several different locations throughout the world.

"The inherent uncertainty of quantum computing offers a unique opportunity to both obfuscate cryptographic computations and create innovative applications that take advantage of this uncertainty," Iyer stated. "This proposal seeks to investigate similar challenges by utilizing NCSA's top-notch computing resources to look into new attacks that target previously impractical supercomputing workloads."

A new path into NCSA's quantum strategy is made possible by this initiative. Núñez-Corrales stated, "Our understanding of the landscape of trust and security in advanced computing is now reconfigured by potential future risks introduced by quantum technologies." Mapping PQC protocol usage will yield important insights for strengthening NSF-funded cyberinfrastructure across the country. We believe this to be a substantial and enduring contribution. Furthermore, as partners in the Illinois Quantum Information Science and Technology Center (IQUIST), our project offers chances to bridge the gap between the security issues associated with the routine operation of world-class supercomputing facilities and the knowledge of campus quantum information science theorists.

Jim Basney, a principal investigator of the NSF-funded SciTokens project and a Principal Research Scientist at NCSA, stated, "This project will contribute significantly to plans for moving SciTokens to PQC, ensuring that our federated ecosystem for authorization on distributed scientific computing infrastructures is ready to withstand quantum computing attacks." "Planning a seamless transition will require an understanding of the effectiveness of token signing and verification, as well as the influence on token length."

The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce completed its primary set of encryption algorithms in August that are intended to withstand cyberattacks by quantum computers. These encryption standards, which are the outcome of eight years of NIST work, are an illustration of the required dedication to future computing security, in which Cao participates through the NIST High Performance Security Working Group.