NIST Workshop on Cybersecurity in a Post-Quantum World

April 2 – April 3, 2015

NIST solicits papers, presentations, case studies, panel proposals, and participation from any interested parties, including researchers, systems architects, vendors, and users. NIST will post the accepted papers and presentations on the workshop web site and include these in a workshop handout. However, no formal workshop proceedings will be published. NIST encourages presentations and reports on preliminary work that participants plan to publish elsewhere. Topics for submissions should include, but are not limited to, the following:

Security Status of Approved Public Key Cryptographic Algorithms

- How does the development of quantum computers affect the security of currently deployed public key algorithms? (E.g., encryption (for key transport), digital signatures, and key agreement)
- How would quantum computers affect other services which rely on public key infrastructure? (E.g. TLS, IPSec, etc.)
- Are there other concerns with the existing public key algorithms that would motivate the development of alternative cryptosystems?
- Are there other advanced computing technologies that could threaten the existing cryptosystems?

Short Term Actions

- How urgent is the need for post-quantum cryptography?
- What changes to applications and protocols could mitigate potential interoperability problems?
- What guidance should NIST provide with respect to post-quantum cryptography?

Conditions for an Early Transition

- What conditions would warrant a transition away from one of the approved public key algorithms?
- What changes to applications and protocols could facilitate such a transition? (E.g., ways of combining existing public key algorithms with newer post-quantum cryptosystems)

Requirements for Post-Quantum Cryptographic Algorithms

- What are desirable properties of post-quantum cryptosystems with regard to security, performance, ease of implementation, and interoperability?
- What are desirable properties of post-quantum cryptosystems with regard to particular applications, such as encryption, digital signatures, key exchange, and message authentication?

Potential Replacement Options

- What are the strengths and weaknesses of the different post-quantum cryptosystems that have been proposed? (E.g., schemes based on lattices, codes, multivariate systems of equations, hash trees, elliptic curve isogenies, Kerberos, etc.)

- How can one gain confidence in the security of these cryptosystems against quantum and classical attacks?
- Are there ways to estimate the real-world performance of a quantum algorithm, without running it on a quantum computer?
- Which of these cryptosystems are mature, and which ones require further development?

Deadlines for submissions are:

- ***Papers, Presentations and Proposals Due: December 15, 2014***
- ***Authors Notified: February 1, 2015***

Submissions should be provided electronically, in PDF, for standard US letter-size paper (8.5 x 11 inches). ***Paper submissions*** must not exceed 15 pages (single space, two column format with 1" margins using a 10 pt or larger font) and have no header or footer text (e.g., no page numbers). ***Proposals for presentations or panels*** should be no longer than five pages; panel proposals should include possible panelists and an indication of which panelists have confirmed participation.

Please submit the following information to pqc2015@nist.gov:

- Name, affiliation, email, phone, postal address for the primary contact author
- First name, last name, and affiliation of each co-author
- The finished paper, presentation or panel proposal in PDF format as an attachment.

All submissions will be acknowledged.