How should the IETF approach Post-Quantum security?

Collecting feedback to define a strategy for mitigating PQ era threats in IETF Protocols

Roman Danyliw

Benjamin Kaduk

SAAG at IETF 111

Perspective of the SEC ADs

Threat

The advent of quantum computers will undermine the security of current (public key) algorithms

Desired Outcome

IETF adapts existing protocols to be able to use openly developed and publicly vetted quantum-resistant crypto primitives

Unknows

- How long do we have?
- How long it will take?
- Exact scope of where and what works needs to be done
- The exact form and fit of the new primitives
- **⇒ (Today's conversation) How to approach producing solutions in the IETF? ⇐**

Perspective of the SEC ADs (2)

- Upgrading protocols to be PQ-compatible is a recurring topic across WGs, inviting a broader conversation
- Work has already started (e.g., PKIX and CMS in the LAMPS WG)
- Protocol upgrades will:
  - Reach into most areas of the IETF and will require coordination
  - Be a partnership – the new algorithms will be defined and vetted based on outside work (IRTF, US NIST, academic community)
- Workload to upgrade existing protocols:
  - Exceeds the bandwidth of the AD-sponsoring process
  - Would be inefficient to run all individually proposal through SecDispatch
- An active WG for a protocol would be best positioned to handle updates
- “Orphan protocols” (without an active maintenance WG) exist
- IETF likely needs a dedicated space to discuss PQ migration topics

Scoping an Approach

- **How do we reason about an approach?**

  [*already enough] … [dedicated ML] … [revisit in SAAG] … [BoF] … [MOPS-style WG]*[1]

- **What is the problem? What work needs to be done?**

  Algorithm Identifiers; SSH, Kerberos, DNSSEC, JOSE, …

[1]https://datatracker.ietf.org/wg/mops/about/

- **How should the work be done?**

  [individually as identified/SecDispatch] … [last-resort CURDLE-style WG][2]

[2]https://github.com/rdanyliw/ietf-pq-maintenance/blob/main/pqm-charter.md

- **When should we start?**

  [now] … [unclear] … [when NIST PQ Round 3 is done]

- **Who do we need to engage beyond the current IETF community?**