Industry Panel Discussion

PQC Workshop

Aug 22, 2019
Panelists and Introductions

• Matt Campagna, Amazon Web Services
• Scott Fluhrer, Cisco
• Brian LaMacchia, Microsoft
• Nataraj (Raj) Nagaratnam, IBM
• Nick Sullivan, Cloudflare
Imagine PQC algorithms are ready to go....

• How long to get PQC into standards (IETF, IEEE, ANS)?

• How long to introduce PQC into products?
  • Early adopters?
  • Stuff that will take forever to change over?
Constraints and Tradeoffs

• What are major barriers to PQC adoption?
  • Existing message formats / sizes?
  • Capacity limits?

• Different algorithms offer different tradeoffs
  • Signature/encryption size vs. public key size
  • Generation vs. verification
  • Bandwidth vs time

• Does your industry need particular tradeoffs?
  • Do any of the current PQC candidates meet requirements?

• Are there some applications that just can’t work with PQC algs?
Hybrid Modes

• Is this a good transition strategy?

• Do we know how to build them?
  • Nice to have something well-analyzed and ready to go.
Algorithm Agility and Fallback

*Crypto agility = ability to turn something *off**

• What applications in your organization can change algorithms quickly?
  • In response to attack...
  • ...or announcement of progress on quantum computers?
• What *can’t* change on the fly?

*When will it be possible to turn off non-PQ algorithms?*
Security Levels, Failure Rates, Etc.

• Is Level 1 secure enough?

• Is Level 5 more than anyone needs?

• Failure rate/performance/security tradeoffs for IND-CPA designs?
IP Issues

• How much will IP issues impede adoption of PQC algorithms?

• Is this a major issue in your organization?

• What can be done in PQC process to minimize those issues?
Other Issues from Panelists

• Transitions
• Hybrid modes
• Constraints and tradeoffs
• Algorithm agility and fallback
• IP issues
• Other stuff?
Audience questions

• Transitions
• Hybrid modes
• Constraints and tradeoffs
• Algorithm agility and fallback
• IP issues
• Other stuff?