Post Quantum Secure Cryptography Discussion

mcgrew@cisco.com

CFRG @ IETF95

About these slides

- The intent of these slides is to facilitate a discussion on post quantum secure cryptography at CFRG @ IETF95
- They do not represent any official position of CFRG or anyone else

What are the PQC use cases?

- Software/Firmware signatures
- Long-term confidentiality
  - Resist "store now, break later "attacks
- Long-term secure remote management
- Other?

Where is PQC on the list of priorities?

Priority	Threat
Robustness	Heartbleed, side channels
Faithfulness	Algorithm substitution
New Curves	ECC authors
Post Quantum Security	**Quantum Computers**
Performance	Non-adoption of crypto

What IETF standards need PQC?

Standard	Use case
SMIME	Software/firmware
TLS	Confidentiality, Mgmt
IPSec	Confidentiality
SSH	Mgmt
Kerberos	Confidentiality
…	…

On PQC adoption timeline is PQC adoption needed?

- Research/standards/implementation/adoption
- Field upgradability
- New algorithms need X years of study
- What old algorithms have PQ security?

What are barriers to PQC adoption?

- Key and signature sizes
- Computational cost
- Lack of algorithm agility

What approaches are needed?

- Supersize symmetric crypto
- Use asymmetric crypto less often
- Hash based signatures
  - Software/firmware signing
- Lattice based encryption
- Lattice based key establishment
  - Ephemeral OK; Static?

Easy

Easy

Not hard

Need review

Need review

Size problems

Inapplicable

PQC Algorithm Standards Work

- NIST
- Fall 2016 Call For Proposals
- Nov 2017 Deadline for submissions
- 3-5 years - Analysis phase
- NIST will report its findings
- 2 years later - Draft standards ready

- ETSI
- PQC Workshops
  - Sept 2016 Toronto
- Algorithms
- QKD

How can CFRG help develop PQC algorithm standards?

- Build community of interest
- Internet PQC problem statement
- Document PQC status of algorithms/protocols
- Coordinate with NIST and other national standards bodies
- Other?

How can CFRG help adoption of PQC in IETF standards?

- Develop recommendations
  - Symmetric: PQC, asymmetric: agile
- Standards review
- Spread awareness

EOF