Current status on PQC

A brief overview on the status of quantum-safe standardization processes, upcoming standards and protocols

Introduction

- update on what to expect during next year
- Questions: drop me an email (elfy@riseup.net, PGP-FP: 0x41B77C52D9DDB5D9) or write me via Matrix (@elfy:possum.city)
- slides for download at https://elfy.dev/static/37c3-pqc-lightning.pdf

Disclaimer: I'm not an academical cryptography expert, I'm doing ~~cyber~~ IT/OT security at my dayjob (DB Systel) and PQC is currently a part of it

Upcoming standards: FIPS (NIST)

Purpose	FIPS Standard Drafts	Standard Name	Algorithm Name
Key Encapsulation	FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism Standard *(ML-KEM)*	CRYSTALS-Kyber
Signing	FIPS 204	Module-Lattice-Based Digital Signature Standard *(ML-DSA)*	CRYSTALS-Dilithium
Signing	FIPS 205	Stateless Hash-Based Digital Signature Standard *(SLH-DSA)*	SPHINCS+

- third signing algorithm (Falcon) will be released in Summer 2024 by NIST
- additional signing algorithms *(Onramp Submissions)* by NIST:
  - 40 candidate algorithms announced in July 2023, currently in review (round 1)
  - final standards expected in several years

Upcoming standards and protocols: IETF

- **TLS 1.3:** draft-ietf-tls-hybrid-design-09 - Hybrid key exchange in TLS 1.3
- **SSH:**
  draft-josefsson-ntruprime-ssh-02 - Secure Shell (SSH) Key Exchange Method Using Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512
  and
  draft-josefsson-ssh-mceliece-00 - Secure Shell Key Exchange Method Using Hybrid Classic McEliece and X25519 with SHA-512: mceliece6688128x25519-sha512
- **IKEv2:**
  raft-kampanakis-ml-kem-ikev2-01 - Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)
- several drafts wrt. **PKI and certificates** (e.g. Composite Signatures For Use In Internet PKI)
- Already standardized "older" stateful hash-based quantum-safe signature algorithms:
  - RFC 8391 - XMSS: eXtended Merkle Signature Scheme
  - RFC 8554 - Leighton-Micali Hash-Based Signatures
- Further information and helpful RFC drafts:
  - GitHub - ietf-wg-pquip/state-of-protocols-and-pqc: A list of the state of IETF protocols and PQC
  - draft-ar-pquip-pqc-engineers-03 - Post-Quantum Cryptography for Engineers
  - draft-ietf-pquip-pqt-hybrid-terminology-01 - Terminology for Post-Quantum Traditional Hybrid Schemes

Real-world usage of PQC

- OpenSSH sshd: ntrup761x25519-sha512@openssh.com hybrid for KeyExchange (beginning with OpenSSH 9.0 from Feb 2022)
- Rosenpass: Wireguard add-on using Classic McEliece 460896 and Kyber-512 for hybrid PQ-security (available since Feb 2023)
- Signal Messenger: PQXDH (Post-Quantum Extended Diffie-Hellman using a X25519/Kyber1024 hybrid (available since Sep 2023)
- Google Chrome: X25519Kyber768 hybrid for key agreement between Google Chrome and Google servers (since Aug 2023)
- GitHub - open-quantum-safe's liboqs C library for quantum-safe algorithms, a Python wrapper is also available

- many software products (both commercial and FOSS) are starting to implement NISTs draft algorithms, some are waiting until the standards are officially passed

General Advice on PQC

- stay up to date
- use PQC where possible and go hybrid where you can
  - capture now, decrypt later attacks can be a problem for data which needs long-term security
  - know your infrastructure and locations/endpoints where (asymmetric) cryptography is in use
  - don't underestimate migration complexity and act as early as possible
- all general advice wrt. “classic” cryptography applies also to PQC

Thanks a lot and see you at 37c3!