Post-Quantum transition: Prepare to changes

Fosdem 2024, February 4

Dmitry Belyavskiy
Principal Software Engineer
Who am I

Dmitry Belyavskiy
Red Hat Principal Software Engineer
Maintain: OpenSSL, OpenSSH

OpenSSL Technical Committee member since 2021

Current work: Post-Quantum transition in Red Hat
Why Post Quantum transition?

There is a consensus that Quantum Computers will break traditional cryptography

   Including deciphering pre-recorded communication

There are world-wide efforts to design and implement Quantum-resistant algorithms
PQ transition challenges - I

We can’t trust classical algorithms
We can’t trust new algorithms
Hybrid solutions: combinations of classical and new algorithms
PQ transition challenges - II

Big keys/signatures

- RSA-3072: 387/384 bytes
- Dilithium2: 1312/2420 bytes

Performance problems

Compatibility problems

Network: TCP/UDP Fragmentation (DNSSec), amplification attacks
PQC: Standard bodies

Algorithms: NIST

Kyber, Dilithium, SPHINX+

Protocols: IETF

PKCS#11: OASIS group
Fedora for PQ experiments

Our choice
Liboqs project
Low-level implementations
A group of projects: OpenSSL provider, OpenSSH

Fedora 39
OpenSSL 3.1, liboqs 0.8, oqsprovider 0.5.1
PQ demo: make it yourself

$ yum install oqs-provider

$ openssl ecparam -out p256.pem -name P-256

$ openssl req -x509 -newkey ec:p256.pem -keyout root.key -out root.crt -subj /CN=localhost -batch -nodes -days 36500 -sha256

$ openssl s_server -key root.key -cert root.crt -trace -provider oqsprovider -groups x25519_kyber768:p384_kyber768

$ openssl s_client -connect localhost:4433 -tls1_3 -trace -provider oqsprovider -groups x25519_kyber768:p384_kyber768
PQ demo: use nginx

$ vim /etc/pki/tls/openssl.cnf
[provider_sect]
derault = default_sect
oqsprovider = oqs_sect
[default_sect]
activate = 1
[oqs_sect]
activate = 1

$ vim /etc/nginx/nginx.conf
ssl_ecdh_curve x25519_kyber768:p384_kyber768;

$ curl --curves x25519_kyber768:p384_kyber768 --cacert root.crt https://myserver/
Future plans

**Container**
No more do-it-yourself

**Fedora rawhide**
Recent versions of OpenSSL, liboqs, oqsprovider
Crypto policy: subpolicy for PQ algorithms

**Upstream work**
OpenSSL, NSS, GnuTLS
SSH: opportunities

OpenSSH implements PQ algorithms
...non-standard PQ algorithms
...to be standardized (IETF)

NIST PQ algorithms: no specifications
OQS-OpenSSH: many PQ algorithms, no contributors
Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHat