Red Hat
Enterprise Linux

Post-Quantum Cryptography: Network protocols

Some problems you may expect with PQ transition

Dmitry Belyavskiy
Principal Software Engineer

CSNOG meeting, Zlin, January 23, 2024

Who I am

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

OpenSSL committer since 2019
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

PQC: Standard bodies

Algorithms: NIST

- Drafts are published, final versions are expected in Q1

Protocols: IETF

- Many documents

PKCS#11: OASIS

New standards: should we trust them?

Classical cryptography expected to be broken

New schemas are not evaluated yet

Nobody is sure

Hybrid solutions

New algorithms - obvious problems

Compatibility problems

Unknown algorithms - middlebox problems

Bigger key/signature size:

- RSA-3072: 387/384 bytes
- Dilithium (2): 1312/2420 bytes

Slower performance

Traditional problems: amplification

Bigger key size => large certificate chains

4k RSA => 22k Dilithium

QUIC: spec-level limitations 3x response/request, extra round-trip

DTLS: spec-level recommendation 3x response/request, nobody implements

Traditional problems: congestion

TCP: Historically: 1 => 10 Maximum Segment Size

CDNs often use bigger values

To avoid extra round-trips, 25 MSS is worth investigation

QUIC: has its own congestion control, worth investigating

DTLS: doesn’t have its own congestion control

DNSSec

Small request, big response => amplification

Too big RRSIGs => don’t fit one packet

ARRF: a proposal to split RRs at application level

Extra research needed

Use Fedora for experiments

Use liboqs project
Side projects: OpenSSH, OpenSSL providers…
Inherits PQClean implementation (chosen by NSS)

Fedora 39: OpenSSL 3.1, liboqs 0.8, oqsprovider 0.5.1

Useful links

Algorithms description

Key Encapsulation: CRYSTALS-Kyber

Signature: CRYSTALS-Dilithium, Falcon, SPHINCS+

Future work

Vision Paper: Do we need to change some things?

Research Agenda for a Post-Quantum DNSSEC

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.

in linkedin.com/company/red-hat

▶ youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat