A testbed to evaluate post-quantum cryptography in DNSSEC

Caspar Schutijser | DINR 2024

04 April 2024

SIDN LABS

PQC for DNSSEC, why?

Quantum computers

Why is PQC for DNSSEC not straightforward?

PQC algorithms have different characteristics in terms of:

- Signature and public key size (problem because of UDP/EDNS buffer size of 1232 bytes, and generally the 64k limit)
- Validation speed
- Signing speed

Evaluation of PQC algorithms in DNSSEC is needed

Which algorithms are suitable for DNSSEC?

What changes to (the deployment of) DNS(SEC), if any, are necessary? Signer setup, authoritatives, resolvers, transport protocols, …

Evaluate, benchmark, prototype

SIDN LABS

PATAD testbed

Post-quantum Algorithm Testing and Analysis for the DNS (PATAD)

Software and **infrastructure**

PATAD software

Patches for DNS(SEC) software to integrate PQC algorithms. Current status: integrated 2 PQC algorithms into PowerDNS, a third is work-in-progress.

Will be made available as open source software.

PATAD infrastructure

Containers and virtual machines (and tooling to deploy them).

"Hosted" version with us but (later) also publicly available code so you can run your own.

Current containers: our PowerDNS authoritative and recursive nameservers. Could also contain your software for your experiments!

Define topology in a file and deploy it: aids reproducibility.

Will be made available as open source software.

SIDN LABS

Next: design empiric evaluation of PQC algorithm

Some ideas:

- Experiment with realistic workloads on different algorithms
- Measure impact on DNSSEC signing and resolvers: signing and validation timings, response times, packet sizes, zone file sizes, …

Any feedback is welcome.

SIDN LABS

Are there any questions?

See https://patad.sidnlabs.nl