A testbed to evaluate quantum-safe cryptography in DNSSEC

Caspar Schutijser
SIDN Labs

Elmer Lastdrager
SIDN Labs

Ralph Koning
SIDN Labs
University of Amsterdam

Cristian Hesselman
SIDN Labs
University of Twente

Domain Name System Security Extensions (DNSSEC) [1] provides authentication and integrity for the Domain Name System (DNS) [9, 10]. To provide those properties, DNSSEC relies on cryptographic signatures [3]. However, algorithms made for quantum computers can break the cryptographic primitives in use today [16], whether based on factorization or on elliptic curves [14]. Although today's publicly-announced quantum computers are not powerful enough to break the cryptographic primitives that we rely on, such computers may become available in the future.

To counter the threat of quantum computers, cryptographers are working on creating *quantum-safe* cryptographic algorithms, or *post-quantum cryptography* (PQC). Such algorithms are hard to solve by both today's computers and quantum computers. The National Institute of Standards and Technology (NIST) coordinates evaluation and standardization efforts on proposed quantum-safe cryptographic algorithms [13]. This process started in 2016 and is still ongoing. It will result in a list of recommended quantum-safe algorithms for signing and encryption.

In DNSSEC, we are interested in algorithms for signing. Although three signing algorithms have been selected as candidates and more are expected, at this moment, there are no standardized quantum-safe signature algorithms. To make sure DNSSEC can continue to provide authentication and integrity for the DNS, it is necessary to make DNSSEC use quantum-safe cryptography.

However, deploying quantum-safe cryptography in DNSSEC is not straightforward. First of all, DNSSEC has stringent requirements when it comes to the characteristics of signature algorithms, for instance related to signature size and validation speed [11]. Furthermore, adoption of new algorithms in the DNSSEC ecosystem takes years since is a complicated process that involves many stakeholders [12].

Empirically evaluating proposed quantum-safe signature schemes in DNSSEC is therefore crucial, so that stakeholders can assess the impact of using such algorithms. To that end, we are building the *Post-quantum Algorithm Testing and Analysis for the DNS* (PATAD) testbed [15]. The goal of the PATAD testbed [1] is to allow us and other DNS stakeholders to prototype and evaluate quantum-safe algorithms in DNSSEC, which allows us to empirically investigate the impact of quantum-safe algorithms on DNSSEC.

The PATAD testbed has two important aspects to it: (1) DNS(SEC) **software** with support for quantum-safe algorithms, and (2) an **infrastructure** that allows us to easily configure various topologies. Next, we will elaborate on both aspects.

Software. In the first version of our testbed, we are using PowerDNS to prototype DNS(SEC) implementations with quantum-safe algorithms. We chose PowerDNS because it can fulfill the role of a *zone signer*, *authoritative name server* and *recursive name server* using one code base. This allows for efficient prototyping of quantum-safe algorithms in the relevant components. At this moment, we have integrated Falcon-512 [5] (inspired by [7] but taking a different approach) and are working on integrating MAYO-1 [2] and SQISign-1 [4].

Infrastructure. To support different experiments, the infrastructure should be easy to reconfigure. We therefore chose a container based approach [8]. Each experiment consists of a series of containers simulating a real world DNS infrastructure: root name servers, authoritative servers for top-level domains (.nl), authoritative servers for domain names (example.nl) and resolvers. An example of an experiment is to (1) run the root name servers using RSA, name servers for .nl using Falcon-512, and the servers of example.nl using ECDSA, and a few resolvers and (2) measure the performance of validating signatures by querying the resolvers.

With some of the building blocks in place, we are now deciding on the types of measurements we want to perform such as evaluating signature generation and validation speed, or simulating key rollovers. The results of our experiments will, ultimately, contribute to answering the research questions posed by an Internet-Draft we are co-authoring, containing a research agenda for a quantum-safe DNSSEC [6].

Acknowledgments. The testbed is being established in collaboration with the SHARQS project at the University of Twente and with SURF, the national research and education network in The Netherlands.

[1] `https://patad.sidnlabs.nl/`

References

[1] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. RFC 4033, IETF, Mar. 2005.

[2] W. Beullens. MAYO: Practical Post-Quantum Signatures from Oil-and-Vinegar Maps. Cryptology ePrint Archive, Paper 2021/1144, 2021. https://eprint.iacr.org/2021/1144.

[3] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, sep 2006.

[4] L. D. Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. Cryptology ePrint Archive, Paper 2020/1240, 2020. https://eprint.iacr.org/2020/1240.

[5] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU. https://falcon-sign.info/.

[6] A. Fregly, R. van Rijswijk-Deij, M. Müller, P. Thomassen, C. Schutijser, and T. Chung. Research Agenda for a Post-Quantum DNSSEC. Internet-Draft draft-fregly-research-agenda-for-pqc-dnssec-00, Internet Engineering Task Force, Sept. 2023. Work in Progress.

[7] M. Grillere, P. Thomassen, and N. Wisiol. FALCON-512 in PowerDNS. https://blog.powerdns.com/2022/04/07/falcon-512-in-powerdns, 2022.

[8] P. S. Kocher. *Microservices and containers*. Addison-Wesley Professional, 2018.

[9] P. Mockapetris. Domain names - concepts and facilities. RFC 1034, IETF, Nov. 1987.

[10] P. Mockapetris. Domain names - implementation and specification. RFC 1035, IETF, Nov. 1987.

[11] M. Müller, J. de Jong, M. van Heesch, B. Overeinder, and R. van Rijswijk-Deij. Retrofitting post-quantum cryptography in internet protocols: a case study of DNSSEC. *SIGCOMM Comput. Commun. Rev.*, 50(4):49–57, oct 2020.

[12] M. Müller, W. Toorop, T. Chung, J. Jansen, and R. van Rijswijk-Deij. The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle. In *Proceedings of the ACM Internet Measurement Conference*, IMC '20, page 295–308, New York, NY, USA, 2020. Association for Computing Machinery.

[13] National Institute of Standards and Technology. Post-Quantum Cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography, 2024. Accessed 16 February 2024.

[14] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In T. Takagi and T. Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 241–270, Cham, 2017. Springer International Publishing.

[15] C. Schutijser, R. Koning, and E. Lastdrager. A quantum-safe cryptography DNSSEC testbed. https://www.sidnlabs.nl/en/news-and-blogs/a-quantum-safe-cryptography-dnssec-testbed, 2023.

[16] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.