Measuring the Performance Impact of NSEC5 (Abstract)

Sharon Goldberg[*] Moni Naor[**] Dimitrios Papadopoulos[‡]
Leonid Reyzin[*] Jan Včelák[§]

[*] Boston University [**] Weizmann Institute [‡] University of Maryland [§] CZ.NIC

While DNSSEC provides authenticity and integrity to the domain name system (DNS), it also introduces a new vulnerability—*zone enumeration* [12, 5, 4, 19]—which allows an adversary that asks a small number of targeted DNS queries (one per record in the zone) to discover the full contents of a zone. An enumerated zone can be used as "a source of probable e-mail addresses for spam, or as a key for multiple WHOIS queries to reveal registrant data that many registries may have legal obligations to protect" [12] (*e.g.,* EU data protection laws [13],[3, pg. 37]), or to create a toehold for more complex attacks. As the Internet of things becomes increasingly ubiquitous, it also becomes increasingly important to keep the names and addresses of these "things" (*e.g.,* thermostats, fridges, baby monitors) away from remote attackers.

NSEC5 was introduced in [8] as an extension to DNSSEC that solves the zone enumeration problem while still remaining secure even if the authoritative nameserver is compromised. (This is in contrast to (1) NSEC3 [12], which is vulnerable to zone enumeration via offline dictionary attacks [5, 19], and (2) "NSEC3 White Lies "[6], and "NSEC3 Black Lies" [16], which solve DNSSEC's zone enumeration problem but assume the authoritative nameserver is trusted to hold the secret DNSSEC zone-signing key (ZSK); thus, if the authoritative is compromised, the security of the zone is compromised as well.) In this work we revisit NSEC5 proposing a modified version based on a custom-made elliptic curve cryptography construction that produces much shorter responses than the originally proposed version. Moreover, we provide the first working implementation of NSEC5-ready authoritative and recursive nameservers, and discuss their performance.

ECC-based NSEC5. The original version of NSEC5 uses a cryptographic construction based on RSA digital signatures. However, recent years have seen the DNSSEC community aiming to replace RSA with elliptic curve cryptography (ECC), in order to shorten the length of DNSSEC responses [11, 17, 14]. Following this trend, we have developed a new provably secure variant of NSEC5 that uses elliptic curve cryptography to produce shorter NSEC5 responses [7]. We have also specified NSEC5 in an IETF Internet draft [18] that describes both its RSA and ECC variants.

NSEC5 implementations. We have also developed the first working implementations of a NSEC5-ready authoritative nameserver and a NSEC5-ready recursive nameserver. Our implementations modified existing DNS software, using Knot DNS [1] for the former and Unbound [2] for the latter. We used these prototypes to evaluate several performance metrics, focusing on DNS response sizes, query resolution time at the authoritative, and validation time at the recursive.

NSEC5 performance. Our preliminary results show that a zone signed with ECDSA with P-256 and using our ECC-based NSEC5 scheme produces negative responses (i.e., NXDOMAIN) that are about half the size of those produced with a 2048-bit RSA ZSK and RSA-based NSEC5. Moreover, ECC-based NSEC5 produces *shorter* responses than today's dominant DNSSEC deployment configuration (NSEC3 with 1024-bit RSA) [15, 10]. The most notable performance overhead of NSEC5 occurs at the authoritative nameserver, since the computation of negative responses involves cryptographic operations. To mitigate this overhead, we introduce a precomputation technique that makes this overhead equivalent to optimized implementations of online signing with "NSEC3 White Lies" (e.g., [9]).

Acknowledgements

This work was supported in part by NSF grants 1012798 and 1012910 and a gift from Verisign Labs.

References

[1] KNOT DNS: High-performance authoritative-only DNS server. `https://www.knot-dns.cz/`.

[2] Unbound: A validating, recursive, and caching DNS resolver. `https://www.unbound.net/`.

[3] Brian Aitken. Interconnect Communications MC/080: DNSSEC Deployment Study. `http://stakeholders.ofcom.org.uk/binaries/internet/domain-name-security.pdf`, 2011.

[4] Jason Bau and John C. Mitchell. A security evaluation of DNSSEC with NSEC3. In *NDSS*, 2010.

[5] Daniel J. Bernstein. NSEC3 walker. `http://dnscurve.org/nsec3walker.html`, 2011.

[6] R. Gieben and W. Mekking. *RFC 7129: Authenticated Denial of Existence in the DNS.* Internet Engineering Task Force (IETF), 2014. `http://tools.ietf.org/html/rfc7129`.

[7] Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, and Leonid Reyzin. NSEC5 from elliptic curves: Provably preventing DNSSEC zone enumeration with shorter responses. Cryptology ePrint Archive, Report 2016/083, 2016. `http://eprint.iacr.org/2016/083`.

[8] Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, Leonid Reyzin, Sachin Vasant, and Asaf Ziv. NSEC5: provably preventing DNSSEC zone enumeration. In *NDSS'15*, 2015.

[9] Olafur Gudmundsson. DNSSEC done right. `https://blog.cloudflare.com/dnssec-done-right`.

[10] Amir Herzberg and Haya Shulman. Fragmentation considered poisonous, or: One-domain-to-rule-them-all. org. In *IEEE Conference on Communications and Network Security (CNS)*, pages 224–232. IEEE, 2013.

[11] Amir Herzberg and Haya Shulman. Cipher-suite negotiation for DNSSEC: Hop-by-hop or end-to-end? *Internet Computing, IEEE*, 19(1):80–84, 2015.

[12] B. Laurie, G. Sisson, R. Arends, and D. Blacka. *RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.* Internet Engineering Task Force (IETF), 2008. `http://tools.ietf.org/html/rfc5155`.

[13] Marcos Sanz. DNSSEC and the zone enumeration. European Internet Forum: `http://www.denic.de/fileadmin/public/events/DNSSEC_testbed/zone-enumeration.pdf`, October 2004.

[14] O. Sury and R. Edmonds. *draft-sury-dnskey-ed25519: Ed25519 for DNSSEC.* Internet Engineering Task Force (IETF), 2015. `https://tools.ietf.org/html/draft-sury-dnskey-ed25519-03`.

[15] Luke Valenta, Shaanan Cohney, Alex Liao, Joshua Fried, Satya Bodduluri, and Nadia Heninger. Factoring as a service. Cryptology ePrint Archive, Report 2015/1000, 2015. `http://eprint.iacr.org/2015/1000`.

[16] F. Valsorda and O. Gudmundsson. *draft-valsorda-dnsop-black-lies-00: Compact DNSSEC Denial of Existence or Black Lies.* Internet Engineering Task Force (IETF), 2016. `https://tools.ietf.org/html/draft-valsorda-dnsop-black-lies-00`.

[17] Roland van Rijswijk-Deij, Anna Sperotto, and Aiko Pras. Making the case for elliptic curves in dnssec. *ACM SIGCOMM Computer Communication Review*, 45(5):13–19, 2015.

[18] J. Včelak, S. Goldberg, and D. Papadopoulos. *draft-vcelak-nsec5-03:NSEC5, DNSSEC Authenticated Denial of Existence.* Internet Engineering Task Force (IETF), 2015. `http://tools.ietf.org/html/draft-vcelak-nsec5-03`.

[19] Matthaus Wander, Lorenz Schwittmann, Christopher Boelmann, and Torben Weis. GPU-Based NSEC3 Hash Breaking. In *IEEE Symp. Network Computing and Applications (NCA)*, 2014.