NSEC5, DNSSEC Authenticated Denial of Existence

draft-vcelak-nsec5-00

Jan Včelák
jan.vcelak@nic.cz

March 26, 2015
IETF 92, Dallas, USA

`http://www.cs.bu.edu/~goldbe/papers/nsec5.html`[1]

[1] Sharon Goldberg, Moni Naor, Dimitrios Papadopoulos, Ondřej Surý, Sachin Vasant, Leonid Reyzin, Jan Včelák, Asaf Ziv

Purpose of NSEC5

- **Prevent zone content enumeration**
- **No private zone signing key on authoritative servers**

- Zone content enumeration:
  - NSEC: possible (easy)
  - NSEC3: harder but still possible (offline attacks)[2,3]
  - NSEC5: **impossible** (cryptographically-proven)[4]
- Possible solutions:
  - NSEC: Minimally Covering NSEC Records[5], requires ZSK
  - NSEC3: NSEC3 White Lies[5], requires ZSK
  - NSEC5: adds new key type, **ZSK not needed**

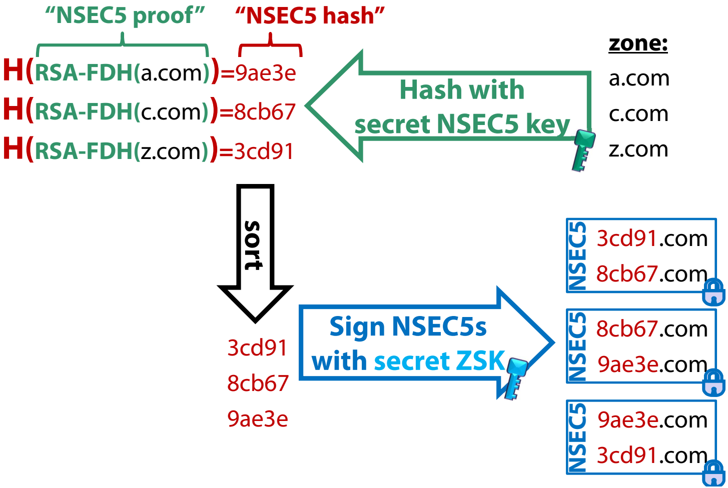
[2] Bernstein D., *Nsec3 walker*, 2011.

[3] Wander M. et al, *GPU-Based NSEC3 Hash Breaking*, in IEEE Symp. Network Computing and Applications, 2014.

[4] Goldberg S. et al, *NSEC5: Provably Preventing DNSSEC Zone Enumeration*, July 2014.

[5] Gieben R. and Mekking W., *Authenticated Denial of Existence in the DNS*, RFC 7129, February 2014.

How NSEC5 Works



"NSEC5 proof" "NSEC5 hash"

H(RSA-FDH(a.com))=9ae3e

H(RSA-FDH(c.com))=8cb67

H(RSA-FDH(z.com))=3cd91

Hash with secret NSEC5 key

zone:

a.com

c.com

z.com

sort

3cd91

8cb67

9ae3e

Sign NSEC5s with secret ZSK

NSEC5 3cd91.com 8cb67.com

NSEC5 8cb67.com 9ae3e.com

NSEC5 9ae3e.com 3cd91.com

NSEC5 proof is RSA-based FDH with SHA-256. NSEC5 hash is SHA-256.

DNS Protocol Changes

- Designed as an alternative for NSEC and NSEC3
- New resource record types:
  - **NSEC5KEY**
    Holds the NSEC5 public key in zone apex
  - **NSEC5**
    Equivalent to NSEC/NSEC3, forms the NSEC5 chain
  - **NSEC5PROOF**
    Synthesised for each NSEC5 inserted into a response
- NSEC5 proofs are very similar to NSEC3 proofs; NSEC5 just adds a Wildcard flag (idea from draft-gieben-nsec4)
- DNSSEC algorithm aliases to signalize NSEC5 support

Current State and Open Issues

- Incomplete: Performance Considerations, NSEC Transitions
- Signalization of NSEC5 support
  - Currently the same as in NSEC3
  - Is there a better way?
- NSEC5 algorithm support (proof and hash)
  - Only FDH-SHA256-SHA256 defined, others in research papers
  - How to add new ones?
- No mechanism to distribute NSEC5 private keys
  - Is it in the scope?

- Current draft: `https://gitlab.labs.nic.cz/knot/nsec5-rfc`