Adding new algorithms to NSEC3

Is it worth it?

Ondřej Surý • ondrej.sury@nic.cz • 26. 3. 2017

NSEC3: Crypto or password hash?

Crypto-secure hash

- Collision resistant
- Fast (quick to compute)
  - Light on resources
- Pre-image resistance
- …

Password hash

- Key Derivation Function
- Collision resistant
  - But the input is usually short
- Expensive on resources
  - To slow down the attacker

NSEC3 Server

- Needs to be fast
  - Computes NSEC3 for all zone misses
- **⇒ Crypto hash**

NSEC3 Attacker

- Needs to be slow
  - So attacker can’t brute force it
- **⇒ Password hash**

No, it’s not worth it!

- SHA1 should be safe in our context (remember only 255 chars as input)
- NSEC3 needs to be fast and slow at the same time