NSEC3 Iteration Consideration draft-hardaker-dnsop-nsec3-guidance

Wes Hardaker

2021-03-11

Outline

NSEC3 Iterations Refresher

Problem space

Solution space

Next steps

NSEC3 Iterations Refresher

NSEC3 – RFC5155

NSEC3 provides an *alternate* "proof of non-existence"

- Discourage zone enumeration
- Provide an "Opt-out" convention for (large) unsigned zone content ranges

NSEC3 at 50km

Method:

- Used instead of clear-text NSEC domainnames
- Uses *N* iterations of a cryptographic hash
- Allows for the (optional) use of a salt

Notes:

- The FQDN is put into the hash
  - Offline dictionary attacks are zone-specific
- Rotating salts only helps once
  - Once you know a name exists: just query for it

Iteration guidance in RFC5155

Maximum limits set in RFC5155:

Key Size	Iterations
1024	150
2048	500
4096	2,500

"This table is based on an approximation of the ratio between the cost of an SHA-1 calculation and the cost of an RSA verification for keys of size 1024 bits (150 to 1), 2048 bits (500 to 1), and 4096 bits (2500 to 1)."

Problem space

Iterations are expensive

- Complex for authoritative engines to calculate
- Complex for validators to calculate
- Everyone suffers

Solution space

We haz experience

Now that we have been doing this for a while

- DNSSEC validation is increasing
  - Let's reduce the penalties
- Define reasonable limits
- Note: *there is no perfect*

Proposal

Recommendations for Zone Publishers

- An *iterations = 0* count
- An empty salt value
- opt-out for large, sparse zones

Recommendations for Validating Resolvers

- SHOULD limit NSEC3 iterations to a maximum of 100
- SHOULD return a SERVFAIL for unsupported sizes
- SHOULD return a new unsupported EDE code

Thus

Key Size	Old Iterations	New Iterations
1024	150	100
2048	500	100
4096	2,500	100

Next steps

WG Adoption?

Is this a document the WG will consider adopting?

- Clearly: details to be hammered out on the list

What is the right track?

- Likely STD to update 5155