NSEC3 iterations etc.

High counts and opt-out considered harmful, avoid fixed salt.

Viktor Dukhovni <ietf-dane@dukhovni.org> and Wes Hardaker

Quick summary

https://datatracker.ietf.org/doc/draft-hardaker-dnsop-nsec3-guidance/

- Iteration counts much above 10 are counter-productive
  - Unnecessary burden on both authoritative servers and validating resolvers
  - Little gain from even 1 extra iteration, 0 is best, but up to ~10 is fine
  - TLDs are changing their settings to 10 or less (e.g., .LA from 150 to 1!)
- Opt-out only for very large, very sparsely-signed zones, perhaps just .COM
  - Avoid otherwise
- Fixed salt is pointless, set to zero length or rotate
  - Adds to cost if long and iteration count is high
  - Mostly harmless if short enough
  - For larger zones, change has same cost as whole-zone signing

The NSEC3 and NSEC3PARAM records

```
NSEC3 alg flags iterations salt next-owner type-bitmap

NSEC3PARAM alg flags' iterations salt
```

- NSEC3PARAM used to replicate settings to secondary servers
- The ***alg(orithm)*** is always 1 (SHA1), this is a feature not a bug
- The only specified ***flags*** bit is 1 == *opt-out*
- The ***flags*'** in NSEC3PARAM is always 0
- Iterations is 16 bits (0–65535) :-(
- Salt to thwart pre-computation, but hashes already salted with zone FQDN
  - hash(*example.com*) != hash(*example.org*)

Why NSEC3

The sensible reasons

- Originally, motivated primarily by the need for opt-out to get .COM signed
  - .COM uses 0 extra iterations, no salt!
- Zone walking with NSEC seen as a deterrent to adoption
  - Fair enough, but first iteration (0 extra) already deters *casual* zone walking
- Salt can further discourage precomputation, if changed regularly

NSEC3 taken too far

- Opt-out makes denial of existence insecure
  - No longer useful to limit zone size for all but the largest zones
    - .ORG mulling moving back to NSEC!
    - Avoid unless managing .COM or similar 10M+ lightly-signed, delegation-mostly zone
- High iterations harms throughput on servers without dedicated GPUs to accelerate SHA1.
  - Determined attackers have access to fast hardware, CT logs, passive DNS datasets, CZDS, ... There are no secret names in DNS, only delayed discovery

Please pass the salt...

Minor concern, mostly good manners...

- The zone FQDN already part of every hash, no global precomputation (rainbow tables)
- Adding salt to this does nothing unless changed often, to deter ongoing brute forcing of the zone through targeted precomputation.
- So either don't bother, or change each time you (whole zone sign)
- When zone signing is incremental, new NSEC3 chain can't be used until generated in full
  - So need time/space to do that while using previous chain
  - Makes changes less likely to happen

Really avoiding zone walking

Lies, damn lies, and statistics

- With on-the-fly signing, minimal NSEC/NSEC3 responses (lies)
  - Return a minimal pair of adjacent names, either or both fictional
  - Sufficient to prove NODATA or NXDOMAIN
  - Leak nothing about other names in the zone
- If your zone is ***that*** sensitive, given enough hardware, lie!
- But is your zone really that secret?
  - CT logs, passive DNS, CZDS, ...