NSEC3 Update

Ben Laurie
<ben@algroup.co.uk>

IETF 64
7 November 2005

NSEC3

- **Latest version:**
  - `http://www.ietf.org/internet-drafts/draft-ietf-dnsext-nsec3-03.txt`

Issue #1

- Signalling
  - **Should NSEC3 be signalled to NSEC3-unaware DNSSEC implementations? I.e. does an NSEC3 zone look bogus or insecure to an unaware resolver?**
  - **We have no strong opinion – there is an independent transition mechanisms I-D. We will use whatever the WG prefers.**

Issue #2

- NSEC3 Transition
  - Is it a requirement that a transition from NSEC to NSEC3 have no period of insecurity?
    - Consensus on list was “no”

Issue #3

- Base 32 encoded sort order was different to binary sort order.
  - Fixed in –03
    - Using RFC 2932 base 32 encoding which preserves sort order

Issue #4

- Hashes create new owner names in a zone – is this a problem?
  - Believe consensus is “no”

Issue #5

- What if a hash and a “real” owner name collide?
  - Believe this is okay
  - No problem having other RR types where there’s an NSEC3

Issue #6

- Potential DoS on resolvers
  - Evil server chooses very high number of iterations
  - We will allow resolvers to set an upper limit for iterations and treat higher numbers as bogus.

Issue #7

- How do secondaries know the NSEC3 parameters?
  - Any parameter set present at the apex will be present in the whole zone

Issue #8

- Rationale
  - Draft needs to include more information about rationale behind design decisions, e.g.
    - Why have a salt?
    - Why have iterations?
  - This will be in the next version

Nominet.uk

Issue #9

- Hash algorithm field is 7 bits – we should share the DS hash algorithm registry which is 8 bits
  - Will be fixed in next version

Issue tracker

Will be available shortly at:

- `http://nsec3.nominet.org.uk/`
- Will be announced on list

Finish

- Questions?