draft-fujiwara-dnsop-nsec-aggressiveuse-00

K. Fujiwara and A. Kato

IETF 92 dnsop WG

4.5 of RFC 4035 defines

- “In theory, a resolver could use wildcards or NSEC RRs to generate positive and negative responses (respectively) until the TTL or signatures on the records in question expire. However, it seems prudent for resolvers to avoid blocking new authoritative data or synthesizing new data on their own. Resolvers that follow this recommendation will have a more consistent view of the namespace”.
- We shoudn’t generate negative response from the cached NSEC RRs
- Our draft proposes to relax this restriction.

Possible Benefits of the proposal

- DNSSEC is not just security anymore
  - Reduces DNS traffic, which was increased by DNSSEC
  - Reduces the damage of random subdomain attacks ("Water Torture" attacks) significantly
  - Reduces queries to Root DNS servers by typo/mistake/some attacks
  - Reduces average RTT to end resolvers

Aggressive use of NSEC/NSEC3

- A full resolver responds NXDOMAIN when the name in question is covered by a NSEC/NSEC3 in the negative cache.
- It responds NODATA when QNAME exactly matches a NSEC/NSEC3 and QTYPE does not exist in the type bitmap.
- The matching procedure applicable to all ancestor domain names of the query name.
- The full resolver is required to check existence of a wildcard (wildcard expansion is also possible)

Considerations

- The purpose of RFC 4035 sentence is to avoid blocking new authoritative data or synthesizing new data on their own
- With this proposal, newly registered resource records may not be used immediately.

- "Inconsistency concern" can be mitigated by limiting effective max RTT
  - RFC 2308 suggests 1 to 3 hours
  - Even 300 seconds, it could reduce queries under random subdomain attack scenario

Other notes

- This technique is called as "NSEC/NSEC3 aggressive negative caching" in Unbound TODO file.
  - since release 0.4, Sep 20, 2007
- Unbound has aggressive negative caching code in its DLV validator.
  - since release 1.1.0, 11 November, 2008

- Fujiwara tested NSEC aggressive caching using Unbound DLV validator code (with small patch)
  - The idea works well to mitigate attacks and reduce queries to Root.