# draft-fujiwara-dnsop-nsec-aggressiveuse-01

K. Fujiwara and A. Kato

IETF 93 dnsop WG

# Overview: Problems

- Random sub-domain attacks (referred to as "Water Torture" attacks) send many non-existent queries to full-service resolvers. The negative cache does not work well
- Root DNS servers receive many non-existent TLD queries
  - Typos, numbers, leaks (.local, .localhost, …)

- Non-existent information in the cache is used if the query name matches only by exact match

# Overview: Basic Idea

- Target full-service resolver receives NSEC RRs
  - Each NSEC RR contains range between adjacent names
  - NSEC RRs are cached
- For example, target domain name = example.com
  - If “**a.example.com in NSEC www.example.com**” is in the cache
  - There is no domain name between **a.example.com** and **www.example.com**
  - (and need to check existence of ***.example.com**)
- Validating resolvers can detect NXDOMAIN error without further queries to authoritative DNS servers by using NSEC information
- However, this idea is discouraged by RFC 4035 (and RFC 2308)

# Overview: Proposal

- Update RFC 4035
  - – DNSSEC enabled full-service resolvers MAY use NSEC/NSEC3 resource records to generate negative responses until their effective TTLs or signatures on the records in question expire.

- Additional updates (to be written in -02)
  - – CD bit MAY be ignored
  - – RFC 2308

# Differences between 00 to 01

- Added reference to DLV RFC 5074 and imported some sentences
- Added Aggressive Negative Caching Flag idea
- Added detailed algorithms (current pseudo code has a bug, I will fix in -02)

# Aggressive negative caching flag

- Problem
  - Auth DNS servers may dynamically generate minimally covering NSEC Records (RFC 4470)
  - Aggressive negative caching provides no benefit in this case
- Proposal
  - Define a new flag AN (support Aggressive Negative caching)
  - A full-service resolver that supports aggressive negative caching SHOULD set AN flag when sending queries to authoritative DNS servers.
- Online signer implementation
  - When an online signer detects random subdomain attacks and a query have AN flag, it can generate NSEC resource records with wider range depending on the attack situation

# Plans to -02

- Add new proposal:
  - CD bit MAY be ignored
    - Because a query with CD bit set disables DNSSEC validation and cannot check NSEC/NSEC3.
    - To allow aggressive negative caching, CD bit need to be ignored while aggressive negative caching process
    - After the process, the CD bit MUST be used as usual
  - Upudate RFC 2308 NCACHE
    - The basic strategy was to cache authoritative error codes keyed by the exact query parameters
  - Refer idea from draft-vixie-dnsext-resimprove
- Fix pseudo code

# Useful ?

- WG Adoption ?