Side effect of DNSSEC: an increase of DS queries
draft-fujiwara-dnsop-ds-query-increase-00.txt

Abstract

A significant increase of periodic DS queries is observed at top level domain (TLD) DNS servers. Currently, almost all of periodic DS queries come from DNSSEC validators and are queries for unsigned delegations. The reason of the increase is low NCACHE TTL value and DS nonexistence. This phenomena is DNSSEC protocol and DNS parameter issue. DS queries will increase as DNSSEC validators will increase.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 09, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Problem statement

Many TLDs have supported DNSSEC. However, many delegations do not have DS resource records. Some of full-resolvers support DNSSEC validation.

A significant increase of DS queries is observed at JP TLD DNS servers. 3.6% of queries are DS queries at JP TLD DNS servers in June, 2013 and they are still increasing. Almost all query names of DS queries are unsigned zone cuts. These DS queries are useless for DNSSEC validation because they are unsigned delegations. Very small number of IP addresses send most of DS queries and the DS queries are periodic.

The conditions of this phenomena are as follows.

- TLD’s TTL value is relatively high, e.g., 86400.
- TLD’s NCACHE TTL value is low, e.g., 900.
- There are many popular query names whose resource record TTLs are low, e.g., 300, and they are unsigned.
- DNSSEC validators receive queries of popular names frequently, e.g. every 5 minutes.

An unsigned delegation does not have a DS RR in its TLD zone. DNSSEC validation process starts when the validator receives a query and it does not exist in the validator’s cache. DNSSEC validators need to
know DS RR existence for each query name. The DS RR nonexistence information is cached within NCACHE TTL. As a result, each DNSSEC validator may send DS queries for TLD DNS servers one zone cut per NCACHE TTL seconds.

JP TLD case, NS, DS and glue TTL is 86400 and NCACHE TTL is 900. There are many popular names which are unsigned domain names and whose TTLs are low. TTL of "www.yahoo.co.jp" A is 60 (CNAME TTL is 900 and TTL of aliased name is 60) and TTL of "www.google.co.jp" A is 300. Busy full-resolvers receives both queries every minutes or more. When a busy full resolver enables DNSSEC validation, it will send "yahoo.co.jp" and "google.co.jp" DS queries every 900 seconds. "yahoo.co.jp" NS and "google.co.jp" NS are cached in a day (86400 seconds). As a result, queries to JP DNS servers may increase 96 (86400 / 900) times at the maximum. This is DNSSEC protocol and parameter issue.

2. Possible affected domain names

Possible affected domain names are delegation centric domain names which support DNSSEC, whose NCACHE TTL is low, and which has popular domain names which are not signed and use low TTL values.

TLDs: com, net, org, jp use 900 as NCACHE TTL value. Magnification is 96 or more.

Reverse DNS: 193.in-addr.arpa uses 3600 as NCACHE TTL value. Magnification is 48.

The root is affected a little because popular TLDs have already been signed and the magnification is not high, 8 or 24 (86400 / 10800 or 86400 / 3600).

3. Possible solutions

There are four approaches to the problem.

1. Lengthen NCACHE TTL value. However, this approach can not stop the increase of DS queries because section 5 of DNS NCACHE [RFC2308] recommends negative cache time limit as values of one to three hours. Lengthening NCACHE TTL value over 10800 is useless. Magnification can only be lowered. (JP case, from 96 to 8 or 24.)

2. Sign all delegations. If all delegations are signed, DS RR are cached. However, a TLD can not control.
3. Lengthen resource record TTL of popular names. However, a TLD can not control.

4. Add dummy DS to unsigned delegations. Dummy DS TTL value is controllable. This proposal requires new digest type. However, using this approach, TLD can not use opt-out technique defined in NSEC3 [RFC5155]. Dummy DS RR will be ignored by traditional DNSSEC validators because Section 5.2 of DNSSEC Protocol [RFC4035] defines that the resolver should treat unknown digest type as no DS RRset exists. BIND 9 and Unbound validators ignored dummy DS RR whose digest type is 255.

4. Possible approaches

A TLD can control its NCACHE TTL value and its zone. Possible approaches for a TLD are careful query analysis, a combination of option 1 and option 4. Step by step approach is possible.

1. Prepare new digest type because it may take long time.

2. Careful query analysis.

3. If DS queries will increase over 50% of queries, then control NCACHE TTL value.

4. If DS queries will increase over 50% of queries, then add dummy DS RRs to popular unsigned domain names.

5. Normative References


Author’s Address
Kazunori Fujiwara
Japan Registry Services Co., Ltd.
Chiyoda First Bldg. East 13F, 3-8-1 Nishi-Kanda
Chiyoda-ku, Tokyo 101-0065
Japan
Phone: +81 3 5215 8451
EMail: fujiwara@jprs.co.jp