DS TTL shortening experience in .JP

APTLD Malaysia Meeting
21 Feb 2014

Yoshiro YONEYA <yoshiro.yoneya@jprs.co.jp>
What is DS?

- Establish a DNSSEC chain of trust by setting in parent zone
- Generated from KSK of child zone, cryptographically equivalent
Background

• One of the biggest concern with registrants and ISPs deploying DNSSEC is name resolution failure
  – DNS name resolution will fail if DNSSEC operation was failed
  – Especially, mismatch of DS in parent zone with DNSKEY in child zone requires urgent recovery between parent and child zone administrators (typically, registrant \(\leftrightarrow\) registrar \(\leftrightarrow\) registry)
  – Even though urgent recovery has done, the influence will remain until DS cache in validators being expired
  – Registrants and ISPs want to shorten this duration
Possible counter measures

1. Flush failed domain’s cache in validators
   - Ad hoc solution
   - Hard to reach each validators’ operators
   - Almost impossible (no scalability)

2. Shorten DS TTL in parent zone
   - Effective solution
   - Moderate value is not widely shared yet
   - Feasible (depends on decision of parent zone admin)
Measurement in .JP

• Dataset and target
  – Query log of 2 out of 7 JP DNS
  – Duration of 9 Sep 2013 – 15 Sep 2013 (typical 1 week)
  – Analyzed DS query ratio
  – DSC graph of 6 out of 7 JP DNS showed the same DS query ratio, so we considered this analysis estimates whole JP DNS

• Analysis results (overview)
  – DS queries / whole DNS queries: about 3.5%
    c.f. Increase of probable DNSSEC Validators and DNSSEC side effect
  – Existing DS queries / whole DS queries: about 0.08%
    Existing DS queries means DS queries to domain names which have DS records
DS query ratio

Date

DS ratio (%)

20130909 20130910 20130911 20130912 20130913 20130914 20130915

Existing DS query ratio (%)

DS ratio

Existing DS ratio

Copyright © 2014 Japan Registry Services Co., Ltd.
Steps to decide moderate DS TTL

1. Similarity with NCACHE TTL
2. Estimation of influence to JP DNS
3. Decision
1. Similarity with NCACHE TTL

- DS TTL can be considered as a duration of influence when name resolution failure occurred by DS registration failure.
- NCACHE TTL is a duration of status when query name did not exist.
- There are similarity between DS and NCACHE regarding name resolution failure.
- NCACHE TTL’s recommended value is 1 hour (3600) to 3 hours (10800) (RFC 2308).
- DS TTL would also be effective within the range above.
2. Estimation of influence to JP DNS

- TTL=86400 (Original)
  - DS query ratio: 3.5%
  - Existing DS query ratio: 0.08%
- TTL=10800 (1/8)
  - DS query ratio: 3.5% (no increase)
  - Existing DS query ratio: 0.60% (~x8)
- TTL=7200 (1/12)
  - DS query ratio: 3.5% (no increase)
  - Existing DS query ratio: 0.90% (~x12)
- TTL=3600 (1/24)
  - DS query ratio: 3.5% (no increase)
  - Existing DS query ratio: 1.78% (~x24)
DS query ratio (Estimation)

- **DS ratio**
- **Ex. DS ratio (3600)**
- **Ex. DS ratio (7200)**
- **Ex. DS ratio (10800)**
- **Existing DS ratio**

Date: 20130909, 20130910, 20130911, 20130912, 20130913, 20130914, 20130915

**Y-axis:** DS query ratio (%)

**X-axis:** Date (20130909 to 20130915)
3. JP’s decision

- Selected the best value for .JP from following conditions

<table>
<thead>
<tr>
<th>Conditions</th>
<th>TTL 10800 (1/8)</th>
<th>TTL 7200 (1/12)</th>
<th>TTL 3600 (1/24)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small impact to JP DNS</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Enough scale to shorten DS TTL</td>
<td>Fair</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Existing DS queries will not increase drastically when DS and/or validators are increased</td>
<td>Good</td>
<td>Good</td>
<td>Fair</td>
</tr>
</tbody>
</table>
Parameters contributes to DS queries

(1/2)

• Number of DS queries per second can be represented by following formula:

\[ Q \approx \frac{(\text{Dom}\# - \text{DS}\#) \times \text{Prob} \times \text{Val}\#}{\text{NCTTL}} + \frac{\text{DS}\# \times \text{Prob} \times \text{Val}\#}{\text{DSTTL}} \]

- \( Q \): DS queries per second
- \( \text{Dom}\#: \) Number of domains in the zone
- \( \text{DS}\#: \) Number of DS registered domains in the zone
- \( \text{Prob}: \) Probability of a domain name reference per second(*)
- \( \text{Val}\#: \) Number of Validators(*)
- \( \text{NCTTL}: \) NCACHE TTL
- \( \text{DSTTL}: \) DS TTL

\[ \Rightarrow Q \approx \text{Prob} \times \text{Val}\# \times \frac{\text{DS}_{\text{TTL}} \times \text{Dom}\# + (\text{NCTTL} - \text{DSTTL}) \times \text{DS}\#}{\text{NCTTL} \times \text{DSTTL}} \]

* Assuming that the probability for each domain name are equivalent and users behavior of each validators are homogeneous
Parameters contribute to DS queries (2/2)

\[
\frac{DS_{TTL} \times \text{Dom} \# + (NC_{TTL} - DS_{TTL}) \times DS \#}{NC_{TTL} \times DS_{TTL}}
\]

- If DS\# / Dom\# is small enough, then DS_{TTL} will not contribute so much
- If DS\# / Dom\# is not small, then DS_{TTL} should be equivalent to or bigger than NC_{TTL}
Conclusion

• JPRS decided to shorten DS TTL from 86400 to 7200
  – This value works fine with JP zone
  – Moderate value will be changed according to increase of validators and DS records
• JPRS shortened DS TTL on 17 Nov 2013 11:00 AM (JST)
  – DS query ratio was not increased (as estimated)
Relative changes of queries (Existing DS)

Date & Time (JST)

Base Point
2013-11-15 10:00:00

Duration of original TTL

Epoch time
2013-11-17 11:00:00

Increase of DS queries (Validator)

Data provided by <http://www.sannet.ne.jp/>
Increase of DS queries (JP DNS)

Epoch time
2013-11-17 11:00:00

Duration of original TTL

Base Point
2013-11-16 00:00:00

Relative changes of queries

Date & Time (JST)

DS
Existing DS
Needs feedback

• Please give your comments based on your similar experiences
  – Would like to have (TLDs’) best practice
Q and A