Encouraging DNSSEC Adoption
What Has Worked and What Hasn't

DNSSEC Workshop @ ICANN45

17 Oct 2012

Yoshiro YONEYA <yoshiro.yoneya@jprs.co.jp>

Background

- .JP launched DNSSEC service at Jan 2011
  - DS registration to .JP zone is available
- 5% of JP Registrars handles DS registration
  - Out of 650 registrars
  - 20% of JP domain names are covered by them
- 0.03% of JP domain names registered DS
  - Out of 1.3M domain names
  - 2% of queries to JP DNS servers is DS query

What we did

- DNSSEC promotion to registrars
  - Private seminars
- DNSSEC examinations with ISPs/Vendors
  - Performance tests
  - Registrar transfer tests
  - Published report to the public (in Japanese/English)
- DNSSEC promotion to the public
  - Joined DNSSEC.JP which was a community activity to promote DNSSEC in Japan
  - Published several kinds of documents to the public (in Japanese)

→ As a result, recognition / understanding to DNSSEC had improved

  - But DNSSEC adoption rate is still very low in registrars / ISPs / registrants

Analysis

- Promotion to Registrars / ISPs / Registrants are not sufficient yet
- Promotion to registrars may be improved by
  - More educations
  - Give incentives
  - … like other TLDs
- How about ISPs / Registrants?

Why ISPs / Registrants are nervous?

- They are recognizing usefulness of DNSSEC
- But, they are also recognizing impact of DNSSEC operational failure
  - Especially, KSK rollover failure
  - Many of DNSSEC operational procedures are automated recently, but KSK rollover is not

Impact of KSK rollover failure

- Cause zone banishing
- ISPs / Registrants will receive a lot of complaint
- Will last until DS cache in validators to be expired
  - DS TTL is under parent zone administrators' control, not under registrants

How to mitigate the impact?

- Some possible countermeasures
  - Ask ISPs (validator operators) to flush the cache
    - Lack of feasibility
  - Register backup DS in parent zone
    - Hard to averaged registrants
  - Shorten DS TTL in parent zone
    - Implemented under some TLDs
- No best practice yet

Discussion

- Need to have best practice for countermeasures against KSK rollover failure
- Shorten DS TTL in parent zone is a candidate as one of the countermeasures
- Preparation for possible failure will encourage ISPs / Registrants to adopt DNSSEC