i.root-servers.net

DNS WG – RIPE 57

Lars-Johan Liman
<liman@autonomica.se>

REPORT FROM IETF 72

AUTONOMICA

Text in *italics* is my own comments on what has happened since the IETF. They are based on a *quick* look at the mailing lists yesterday.

(The leading word is *quick*! Expect errors.)

DNSEXT

Co-chairs:
Ólafur Guðmundsson
Andrew Sullivan

draft-ietf-dnsext-forgery-resilience

Measures for making DNS more resilient against forged answers

- Passed WGLC
- New version published
- Make sure WGLC issues were addressed

After: Discussion on the list ratholed, Ólafur taking new grip on discussion

draft-ietf-dnsext-dnssec-rsasha256

Use of SHA-256 algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC

- New key types for DNSSEC.
- There were no comments.

After: WGLC was sent out in mid-August, some issues on the list, new version few days ago.

draft-ietf-dnsext-dnssec-bis-updates

Clarifications and Implementation Notes for DNSSEC"

- Chairs want WGLC in Sept, but need consensus on the list first.
- Action point: Andrew Sullivan to create a discussion thread on the list.

After: Was done, died off, no WGLC yet.

draft-ietf-dnsext-rfc2671bis-edns0

- The editor claims that this document is done.
- Action point: Ólafur to send the document to WGLC when the previous document WGLC ends.

After: Since previous didn't hit WGLC, I-D now expired.

draft-ietf-dnsext-tsig-md5-deprecated

Deprecate HMAC MD5 in TSIG

- Requested that the text should say “no longer required” rather than “deprecated”.
- Noted that there is no good place to record requirement levels. Therefore is not ready for WGLC, even if the document as such is OK.

draft-ietf-dnsext-tsig-md5-deprecated

- We need to modify the IANA registry to contain that type of information.
- Action point: Peter Koch to send text regarding requirement levels in the IANA registry.

After: Hasn't happened yet – or has happened in some other venue than DNSEXT.

draft-ietf-dnsext-axfr-clarify

- Needs section on differences between
  - loading a zone into a master
  - transferring a zone in a zone transfer.
- Action point: Ed Lewis to write a scratch proposal on text to address this issue.

After: Text was sent, discussion, died out.

Proposed WG work

draft-crocker-dnssec-algo-signal

- Signaling Cryptographic Algorithm Understanding in DNSSEC
- The document has two goals:
  - to reduce the response size between a resolver and an authoritative server; and
  - to signal when new algorithms are deployed.
- Action point: Scott Rose req. adoption.

After: Request in Aug. No sign of adoption.

Clarif. RFC 1123 TLD labels

- TLD labels are always alphabetic per RFC 1123. Needs update. IDN TLDs!
- Issues: protocol specification, jumping digits, registration procedures (IANA), old implementations, spec. for “label” differs from doc. to doc.
- M Larson and L-J Liman to draft new doc.
- *After: hasn't happened yet ... <blush!>*

Dynamic zones and DNSSEC

- Mark is looking for group of people to work on this, and investigate the problems.
- Ed Lewis noted that he had written something up once and was willing to contribute it to the discussion.

Discussion: further forgery resilience work

- OG urged the audience to deploy draft-ietf-dnsext-forgery-resilience without delay, even though it has just passed WGLC.
- discussion on dns0x20
- Need more proposals in I-Ds, then decide which to adopt.

Any Other Business

- Roy Arends and John Dickinson gave a short demonstration of a proof-of-concept program that infects a cache, which, in the very limited environment, succeeded in a matter of seconds.

This is scaaaary stuff, folks! ☹

DNSOP

Co-chairs:
Rob Austein
Peter Koch

draft-ietf-dnsop-reflectors-are-evil

- All issues resolved except one IESG comment.
- AD holding document because of comments from Paul Hoffman, but was is not aware of that and was happy with current version.
- AD (present) would call off DISCUSS.

After: published as RFC 5358/BCP.

draft-ietf-dnsop-default-local-zones

Locally-served DNS Zones

- Waiting for PROTO Write-Up.

After: No action seen on list.

draft-ietf-dnsop-reverse-mapping-considerations

- Waiting for PROTO Write-Up

After: No action seen on list, now expired.

WG Charter

- "Performance and measurement" - overlap?
  - Performance Metrics for Other Layers WG?
  - Benchmarking Methodology WG?
  - DNSOP chairs talking with chair of these WGs.
- New draft charter after IETF.

After: Hasn't happened yet.

draft-ietf-dnsop-respsize

DNS Referral Response Size Issues

- Awaiting WGLC

After: Hasn't happened yet.

draft-ietf-dnsop-as112-*

draft-ietf-dnsop-as112-ops

draft-ietf-dnsop-as112-under-attack-help-help

- Awaiting WGLC
- Need to be revived for WGLC, no other hurdles.

After: Neither has happened yet.

draft-ietf-dnsop-dnssec-trust-anchor

DNSSEC Trust Anchor Configuration and Maintenance

- All(?) comments are addressed in -02.
- WGLC “Real Soon Now”

After: A couple of questions back in Aug, but since then, nothing.

draft-ietf-dnsop-resolver-priming

Initializing a DNS Resolver with Priming Queries

- Several changes proposed, e.g.:
  - Aligning TTL
    - A/AAAA
    - With SOA
    - With root-servers.net zone.
  - If not fit in 512b, mix A/AAAA glue records.

Current & New Topics

Design Team Deliverable

- Name Server Configuration Protocol DT
- Report = req. document.

  draft-hardaker-dnsops-name-server-management-reqs-03.txt
- Make requirements WG work item *(Done)*
- Disband design team (DCOMA) *(Done)*
- Start working! *(Getting there ...)*

DNSSEC Oper. Practices bis

- Document by Paul Hoffman.
- Proposal to revise RFC 4641
- Idea is result from .ORG DNSSEC review, PIR used the RFC and it was not good!
- Proposed to treat current document as draft and start an “issues list”.

draft-jabley-dnsop-missing-mname

Indicating Non-Availability of Dynamic Updates in the DNS

- Comments:
  - Document predicated on broken update clients.
  - Is protocol change ➔ DNSEXT.
- Update traffic may be real problem.
- All DNS chairs will decide where to put.

draft-kerr-dnsop-edns0-penetration

EDNS(0) Support in Authority Servers

- Methods for and results from experiment trying to measure amount of EDNS(0) support.
  - 16.0% of authority-only servers are defective
  - 94.4% of non-defective authority-only servers are EDNS0-capable.
- Results questioned. “Measure what how?”