IETF Hackathon
DNS/DELEG/Generalized notifications

IETF 119
16–17 March 2024
Brisbane, Australia

Compact Denial of Existence for DNSSEC

- `draft-ietf-dnsop-compact-denial-of-existence-03`
- Goal: less signatures to compute for dynamic signers
- No more NXDOMAIN, every denial of existence is NODATA
- Nothing to do on the resolver side (except if they want to restore NXDOMAIN)
- Hackathon work: two authoritative name servers

Work done and lessons

- adns_server https://github.com/shuque/adns_server
- Drink https://framagit.org/bortzmeyer/drink/
- No problem, CDE is simple
- Even the optional EDNS signaled RCODE restoration is straightforward
- Extended DNS Error for the responses?
- What about non-DNSSEC clients?

Shumon Huque & Stéphane Bortzmeyer

DELEG

- Discussions!
- draft-dnsop-deleg editing
- Preparation for BOF (Tuesday 9:30am)

Ralf Weber, David Lawrence & David Blacka

- PoC of DNSKEY’s DELEG flag in CoreDNS

Manu Bretelle

DELEG

- DELEG introduces a new way for referrals
- But the old, legacy way can never go!
- Will we ever sunset IPv4, when all is in IPv6 ?
- DELEG can be the source for legacy delegations!
- ldns-signzone -D option that adds the legacy NS RRset and glue extracted from the DELEG and SVCB records (in case of alias)

Willem Toorop https://github.com/NLnetLabs/ldns/tree/ietf119/DELEG

DSYNC: Delegation Synchronization

- The problem space of automating sync of delegation information is… well known
- Drafts:
  - draft-ietf-dnsop-generalized-notify-01
  - draft-johani-dnsop-delegation-mgmt-via-ddns-02
- Key change from previous efforts:
  - Proposal for locating where to send updates, allowing child-specific endpoints (e.g., registrar)
  - generic: works for notifications / DNS Updates / …

DSYNC: What got done

- Hacked Johan's tdns auth nameserver
  - hidden primary with signing BIND in front
  - implemented endpoint discovery via DSYNC records (using Knot Resolver)
- Deployed setup under parent.axfr.net with two children (signed and unsigned)
- **Status:** partial support for automated updates via DNS Update
  - Extension to notifications will be straightforward

DSYNC: What we learned

- There are many steps to this.
- On the …
  - child end: lots of analysis to compute exact status/diffs;
  - parent: lots of validation/policy checks
- Skillset at the table helpfully complementary
- Improved understanding of bootstrap for unsigned case

➢ **Next:** continue work on this. Goal is a full working system, automating both child and parent, for generalized notifications + CDS/CSYNC processing and DNS Updates

Wrap Up

Team members:

Shumon Huque
Stéphane Bortzmeyer
Ralf Weber
Dave Lawrence
David Blacka
Manu Bretelle
Willem Toorop
Peter Thomassen

Lars-Johan Liman
Johan Stenstam
Paul Hoffman
Geoff Huston
Joao Damas
Benno Overeinder
Many more…..