DNSSEC Automation Observations

Observations

by Mark Elkins <mje@posix.co.za>

ICANN-72 - October 2021

First talk – as a Registry

#1 - "Gather the Children DS" (ICANN-69)

Just for the EDU.ZA zone (Non EPP, Web based management)

- Now at 167 Domain (20 added, 3 deleted)
- 5 new signed domains –> 12 domains (7%) 🙁
- No bad Nameserver records 🙂

First talk - actions

Have contacted all additional 7 domains that are with Cloudflare – where auto-DNSSEC is available. Some success...

- 10 domains use Cloudflare

  - 4 are DNSSEC Signed

- 8 domains use Posix – all are signed

Second talk – as a Registrar

#2 - "Registrar DS management for DNS providers" (ICANN-70)

- Down from 1561 to 1514 domains (Covid?)

- All Domains with locally hosted DNS are signed when possible

- Almost no bad Nameserver records

Context

- Non-ICANN accredited Registrar
- Accredited for ZA and some other ccTLD's
- Reseller for DNS Africa (fully automated with EPP)
- Reseller via others
- 720 possible TLD's
- 1514 "Domains"
  - 521 managed by internal DNS (I run the DNS Zone)
    - 366 Domains are signed – 70%
  - 43 have no Zone – e.g. Web site for sub-domain
  - 949 managed by external DNS operators (27% signed)
    - 163 Domains use Cloudflare – only 9 are not signed
    - 106 other domains are signed
- 635 signed of 1470 potentially sign-able domains (43% signed)

DNSSEC Management

How this works

- A php script runs at 3:30am, digs every "remote" domain for CDS
  - existing signed via DNSSEC aware resolver
  - all non-signed via TCP to the first listed Nameserver
- CDS 0 0 0 00 (null record) – will remove all DS records
- Mirrors the CDS to DS records
- New CDS records are recorded and if no changes after three days, are deemed to be valid

Cloudflare observations

- They sign with Algorithm 13

- They only add the CDS Record "DS-256" (Digest Type 2)

- They always use "Key Tag" 2371

  - A short numeric value which can help quickly identify the referenced DNSKEY record.

- They support the addition of a CDS Null record to signify that DNSSEC has been withdrawn

Thank you

Questions?

Mark Elkins

mje@posix.co.za