FRED & DNSSEC automation

Jaromir Talir • jaromir.talir@nic.cz • 5.11.2016

Agenda

- DNSSEC automation overview
- How to implement it in FRED
- Obstacles
- Future

DNSSEC automation

- DNSSEC brought slightly more effort for sysadmins
  - Re-signing because of expiring signatures
  - Rolling keys as a good security practice
- For wide DNSSEC adoption, good tool is necessity!
  - OpenDNSSEC
  - Bind inline signing
  - KnotDNS automated signing

DNSSEC automation

- Still KSK rollover is generally manual effort with registrar cooperation
  - Log in to registrar, fill the form with new key
  - After some time log in again and remove old key
- RFC 7344 - Automating DNSSEC Delegation Trust Maintenance – Sep 2014
  - Publishing new keys as CDS/CDNSKEY resource records
  - Responsible entity will do update based on verified DNSSEC response

DNSSEC automation

- How is RFC 7344 supported in tools?
  - OpenDNSSEC-CDS (branch, last commit 2013)
  - KnotDNS – expected early in 2017
  - Bind 9.11 – released 5.10.2016 (month ago!)
    - New automation tool dnssec-keymgr
    - Supposed to have full CDS/CDNSKEY support
    - At the end, only partially supported (not in dnssec-keymgr but only in dnssec-settime)
- Bind 9.11 is usable with some tweaks

FRED

- Open source registry - https://fred.nic.cz
- Developed by CZ.NIC since 2006
  - Used for 0.2.4.E164.ARPA, CZ, CO.CZ, IT.AO, CO.AO, TZ, FO, CR, AL, MK
- News in 2016
  - Deployment in MW (Malawi) and AR (Argentina)
  - RDAP implementation (RDAP for CZ still single in IANA registry http://data.iana.org/rdap/dns.json)

FRED & DNSSEC

- Support for key sharing by introducing KeySet as first class object:
  - Collection of DNSKEY resource records
  - EPP extension for registrars
  - Dedicated registrar
  - Associated technical contacts
- Registrars doesn’t upload DS but DNSKEY

FRED & DNSSEC automation

- Prototype automation script to be invoked regularly via cron
  - Using fred-client python library & dnspython
  - Get CDNSKEY via DNSSEC validating resolver
  - Call update_keyset via EPP
- Deployment scenarios
  - Registry modifies objects of registrars
  - Registrars will deploy this service
  - Registry will be the registrar for keysets

Registry modifies objects of registrars

- Registration rules say the data of domains, contacts, nssets and keysets are changed only via registrars
  - Explicit exceptions for implementation of court decisions and optimization purposes
- May be changed, but it's a long term process

Registrars will deploy this service

- Registrars could do it already… if the knew
- Topic scheduled for next regular meeting
- Informal discussions with a few show some support
  - Competitive advantage?

Registry will be the registrar for keysets

- Solution supported by architecture
- We have done it already
  - Our identity service mojeID is nothing more than registrar for validated contacts
- Operational cost is minimized by automation
- Still there is bootstrap issue – currently only registrar of domain may associate domain with keyset

Obstacles

- Shared KeySets
  - Wait until all domains has the same CDNSKEY
  - Configuration of signaling domain – do changes when this domain has new CDNSKEY
- Bootstrap
  - Registrants must create initial KeySet manually
- Timing
  - Anytime in between zone file generation (1/2h)

Future

- Currently all three scenarios looks viable (may change)
- Internal prototype is almost finished
- Some issues may be resolved by implementation of draft-latour-dnsoperator-to-rrr-protocol

Thank You

Jaromir Talir • jaromir.talir@nic.cz

CZ DOMAIN REGISTRY