DNSSEC automated tools

DNSSEC Workshop

Ondrej Filip • ondrej.filip@nic.cz
20 Nov 2013 • Buenos Aires

CZ DOMAIN REGISTRY

CZ.NIC, CZ.NIC Labs

- About 1.1M domains
- Not just domain registry for .cz
- R&D department – CZ.NIC Labs
- BIRD, DNSSEC Add-on, Knot DNS, ...
- Check http://labs.nic.cz
- Registry software FRED

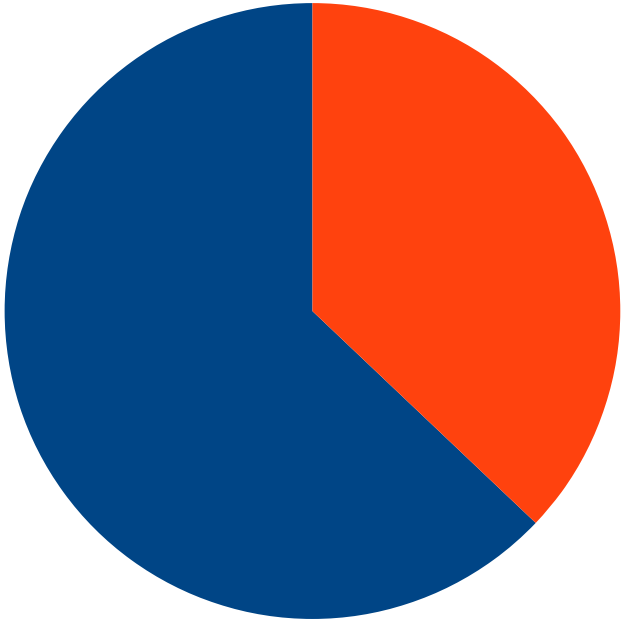
What is FRED

FRED

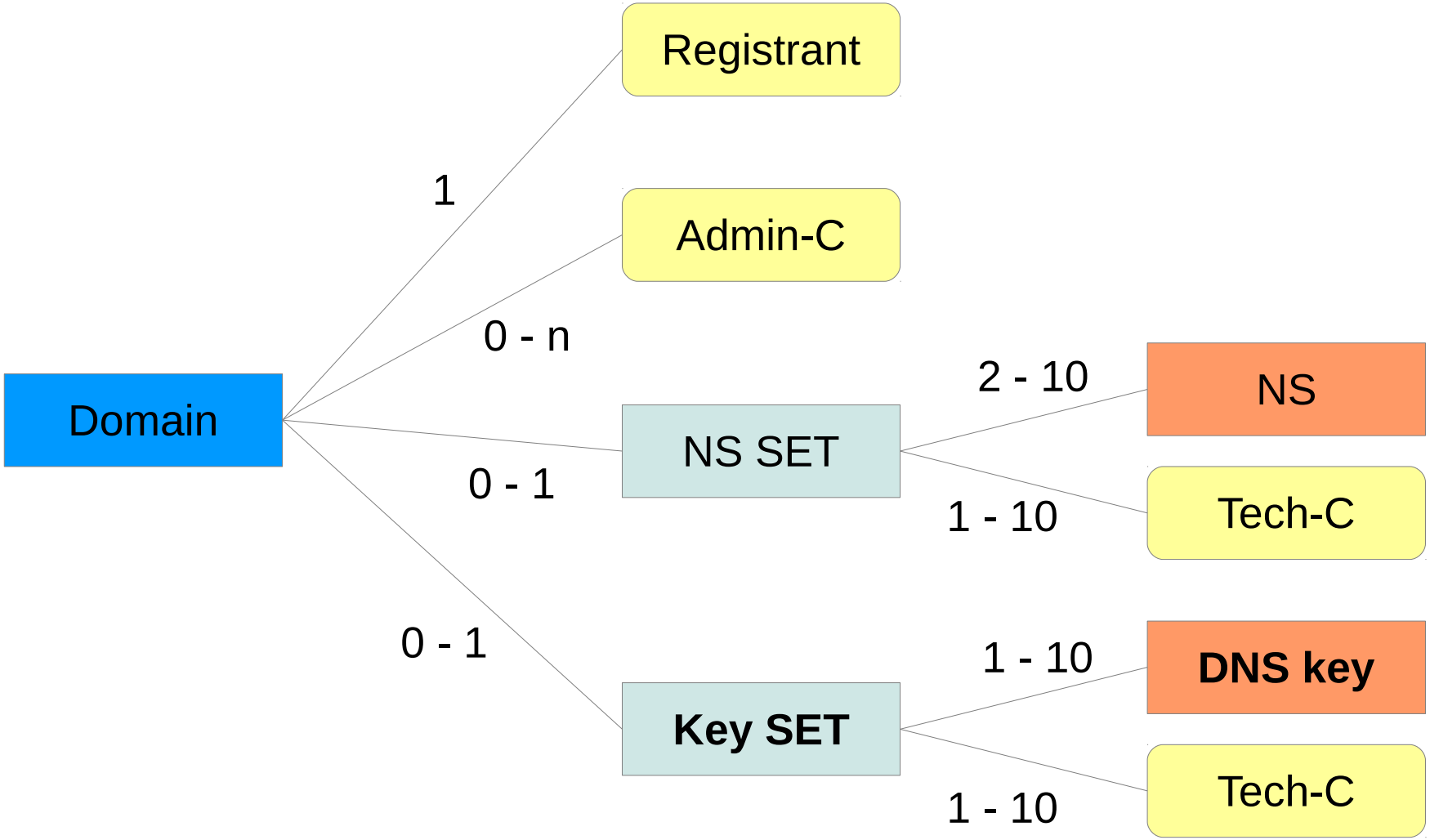
- Open source registry software running .CZ developed by CZ.NIC
- DNSSEC ready – fully automated
- Deployed at CZ, AO, TZ, CR, FO, EE, AL
- http://fred.nic.cz
- Presented on DNSSEC WS in Durban

DNSSEC.CZ

- High DNSSEC prenetration
- About 37% signed (405k from 1.092k)
- Check numbers on http://www.nic.cz



Data structure - keyset



Keys can be reused!

Issue

- DNSSEC domains get signed
- And they become bogus
  - Transfers between registrars
  - Negligence
- Some percentage of errors
  - The more domains are signed the more absolute number of failures you get
- Problem with validating ISPs – disadvantage compared to non-validating

First round

- EPP change of nameservers (NSSET)
  - Reset the secure delegation (KEYSET = DS)
  - Need to explicitly (re-)add the secure delegation
- Helps some cases
  - Transfer between registrars with DNS change
  - Transfer from DNSSEC-aware to DNSSEC-ignorant
- Some not
  - "Smart" registrar system
  - Only registrar → registrar transfers (and the old one stops supporting the domain)

Second round

- Detect bogus DNSSEC signatures
- Remove secure delegation when:
  - DS exists (obviously)
  - Nameservers can be reached (not LAME)
  - Validation fails for 5 consecutive days
    - No DNSKEY in the zone
    - Bogus DNSSEC signature
    - DNSSEC signature has expired
    - Trace from root zone also fails
  - Reset counter if any other condition is met

Second round (cont.)

- Registrar can choose the action:
  - Receive the list of validation failures (minority)
  - Let us handle the failures (delete KEYSET)
- Per registrar/KEYSET rule
  - Handle only well-known KEYSETs (mass hosting)
  - Rest is handled manually by help-desk (call to domain holder)
- Stop if
  - There's more than 100 secure delegations to delete
  - Any other error or unknown condition

Numbers

- End of August 2011
  - ~3000 bogus DNSSEC domains (2%)
  - Registrars fix their EPP scripts and interface
- September 2011
  - ~1200 bogus DNSSEC domains (0,8%)
  - Some more fixing at registrar side
  - Some registrants contacted, mostly they don't care
    - But some fixed or at least removed the bogus signatures
- Since that
- ~9 bogus DNSSEC domains daily (2012, 2013)

Conclusion

- Some percentage of signed domains does not resolve – errors, negligence, …
- About 2% in .cz
- Disadvantage for validating ISPs
- Automatic removal of DNSKEY reference (DS)
- This effort helped and many ISP started to validate – almost all major ISPs/cell phone operator etc.

Thank You!

Ondrej Filip • ondrej.filip@nic.cz • http://www.nic.cz
http://fred.nic.cz