Handling bogus DNSSEC

CZ.NIC / www.nic.cz
Ondrej Filip & Ondrej Sury
ondrej@nic.cz
Oct 24 2011, Dakar, ICANN, Tech Day
DNSSEC penetration at .CZ

- About 17% domains is signed
- That means ~ 145,000 domains! (of 856,000)
- Check numbers at http://www.nic.cz
DNSSEC

- Three registrars enabled DNSSEC by default – domains on their DNS servers
- Well communicated – very good media coverage
- Some more to come...

- 11 registrars have more than 100 signed domains each – more than 90% of market share
Keys can be reused!
Problem

- 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
Some boring numbers

- End of August
  - ~3000 bogus DNSSEC domains (2%)
  - Registrars fix their EPP scripts and interface

- September
  - ~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

- October
  - ~10 bogus DNSSEC domains daily
Some nicer numbers (forecast)
Conclusion

• Some percentage of signed domains does not resolved – error, negligence, …
  – About 2% in .cz
• Disadvantage for validating ISPs
• Automatic removal of DNSKEY reference (DS)

• Czech Republic - the most secured DNS in the world :-) - and we go on...
Thank you

Questions?

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