DNSSEC security without maintenance

... with the right software and registry

Petr Špaček • petr.spacek@nic.cz • 2019-02-03
DNSSEC? Who cares?

Use of DNSSEC Validation for World (XA)

Average Interval (days) 30

Show Google PDNS Use
Hide Regional Use
Redraw

Validating: 18.71 | 01:00 January 26, 2019

https://stats.labs.apnic.net/dnssec/XA

~ 19 %
DNSSEC? Who cares in Europe?

Use of DNSSEC Validation for Europe (XE)

Average Interval (days)
30

Show Google PDNS Use
Hide Regional Use
Redraw Region Map for Europe (150)

DNSSEC Validation Capability Metrics
https://stats.labs.apnic.net/dnssec/XE

~ 24 %

https://stats.labs.apnic.net/dnssec/XE
DNSSEC? Who cares in CZ?

Use of DNSSEC Validation for Czech Republic (CZ)

Average Interval (days)
30

Use of DNSSEC Validation for Czech Republic (CZ)

https://stats.labs.apnic.net/dnssec/CZ

~ 63 %
Where is a problem?

- DNSSEC requires zone content maintenance
  - more work compared to insecure DNS

- Signatures with timestamps
  
  . RRSIG DNSKEY 8 0 172800
  201902110000000 2019012100000000 ...

- Key propagation
  
  • cz. DS 20237 13 2 CFF0F3ECDBC52...
Maintenance?!
DNSSEC maintenance: signatures

- Refreshing signatures (timestamps)
- **fully automated**
  - Knot DNS, BIND, PowerDNS, OpenDNSSEC,
DNSSEC maintenance: keys

- Key propagation
  - **harder problem** – multiple parties
  - sub-optimal support from registrars
  - DNS providers have no relationship with registrar/registry
  - Domain holders do not care
Standards to the rescue

- RFC 7344 - Automating DNSSEC Delegation Trust Maintenance - September 2014
  - cz. CDS 20237 13 2 CFF0F3ECDBC52...
- RFC 8078 - Managing DS Records from the Parent via CDS/CDNSKEY – March 2017
  - cz. CDS 0 0 0 0 0
- draft-ietf-regext-dnsoperator-to-rrr-protocol - Third Party DNS operator to Registrars/Registries Protocol
Standards to the rescue

- DS
- DNSKEY
- CDS
- parent
- child
DNSSEC Trust Maintenance: registry

1. Enable DNSSEC
2. Serve CDS record for domain
3. Checks for CDS for domain
4. Verify ownership and validity of CDS
5. Serve DS record for domain
6. Domain Secured
Implementation in registries

- Supported by
  - .ch
  - .cr
  - .cz
  - .li
- More coming
- Ask your registry!
Implementation in software

- OpenDNSSEC – planned
- PowerDNS – generates CDS RR, manual rollover using pdnsutil
- BIND 9.13 – generates CDS RR, manual rollover using dnssec-keymgr
  - BIND 9.15 – more automation planned
- Knot DNS 2.6+ – generates CDS RR, rolls automatically (as configured)
Key propagation in

- KSK submission via CDS/CDNSKEY
- Periodic checks for DS existence via set of configured nameservers
  - Authoritative nameservers
  - And/or DNSSEC validating resolver
  - (all must see DS)
- Alternative: simple timeout
Configuration example

remote:
- id: auth
  address: [ 198.51.100.5 ]
# resolvers
- id: local
  address: [ 192.0.2.1 ]
- id: foreign
  address: [ 1.1.1.1 ]

submission:
- id: upstream
  parent: [ auth, local, foreign ]
  check-interval: 600 s

policy:
- id: ecdsa
  ksk-lifetime: 14d
  ksk-submission: upstream

template:
- id: "default"
  dnssec-signing: on
  dnssec-policy: ecdsa

zones:
- domain: dnssec.cz
remote:
  - id: auth
    address: [ 198.51.100.5 ]
  
# resolvers
  - id: local
    address: [ 192.0.2.1 ]
  - id: foreign
    address: [ 1.1.1.1 ]

submission:
  - id: upstream

policy:
  - id: ecdsa
    ksk-lifetime: 14d
    ksk-submission: upstream

template:
  - id: "default"
    dnssec-signing: on
    dnssec-policy: ecdsa

zones:
  - domain: dnssec.cz

check-interval: 600 s

parent: [ auth, local, foreign ]
Configuration example

remote:
- id: auth
  address: [ 198.51.100.5 ]

# resolvers
- id: local
  address: [ 192.0.2.1 ]
- id: foreign
  address: [ 1.1.1.1 ]

submission:
- id: upstream
  parent: [ auth, local, foreign ]
  check-interval: 600 s

policy:
- id: ecdsa
  ksk-lifetime: 14d
  ksk-submission: upstream

template:
- id: "default"
  dnssec-signing: on
  dnssec-policy: ecdsa

zones:
- domain: dnssec.cz

# resolvers
- id: auth
  address: [ 198.51.100.5 ]
- id: local
  address: [ 192.0.2.1 ]
- id: foreign
  address: [ 1.1.1.1 ]

# resolvers
- id: upstream
  parent: [ auth, local, foreign ]
  check-interval: 600 s

policy:
- id: ecdsa
  ksk-lifetime: 14d
  ksk-submission: upstream

template:
- id: "default"
  dnssec-signing: on
  dnssec-policy: ecdsa

zones:
- domain: dnssec.cz
Key maintenance: logging

1) 2017-10-24T15:41:22 notice: [dnssec.cz.] DNSSEC, KSK submission, waiting for confirmation

2) Knot detects the updated parent’s DS record
   • + waits for DS’s TTL before retiring the old key

3) 2017-10-24T20:00:00 notice: [dnssec.cz.] DNSSEC, KSK submission, confirmed
Other relevant features

- DS deletion via CDS 000000
- Structured logging for key events
  - custom hooks
- Automatic algorithm rollovers
- Push for DS RR (DNS Update) coming ...
Summary

- DNSSEC is becoming easy (finally!)
- Ask your registry or registrar for CDS/CDNSKEY support
- Update your software
- Sign your zones, please ;-)
Backup slides

CDS/CDNSKEY implementation in CZ
CDNSKEY scanning

- Daily scanning all domains in zone for CDNSKEY records
  - Takes about 3 hours for .CZ
- Three categories of domains:
  - Without KeySet
  - With automatically generated KeySet
  - With legacy KeySet created by a registrar
Domains without KeySet

- Scanning all authoritative nameservers from registry database via TCP queries
- When CDNSKEY is found, technical contact is informed via e-mail
- Keep scanning for 7 more days
- If results are always the same (and it is not DS deletion), new KeySet is created and linked to a domain
  - Domain holder (via notify e-mail) and registrar (via EPP) are notified
Domains with automatic KeySet

- Scan for CDNSKEY via local resolver, DNSSEC is validated inside scanner
- If CDNSKEY is found, do as requested
  - Update KeySet with new DNSKEY or
  - Remove KeySet (notification of domain holder and registrar)
- Technical contact is informed via e-mail
Domains with legacy KeySet

- Scan for CDNSKEY via local resolver, DNSSEC is validated inside scanner
- If CDNSKEY is found, do as requested
  - Create new automatic KeySet and swap it in domain or
  - Remove KeySet
- Technical contact is informed via e-mail
- Domain holder (via notify e-mail) and registrar (via EPP) are notified