DNSSEC Bootstrapping

IETF 114 – Hackathon

23-24 July 2022

Philadelphia, Pennsylvania

Hackathon Plan

- Draft: draft-ietf-dnsop-dnssec-bootstrapping
- Requires co-publishing the target zone's CDS/CDNSKEY records at a subdomain of the nameserver's hostname
- Example: Bootstrapping `example.co.uk` via `ns1.desec.io` requires:

  `_dsboot.example.co.uk._signal.ns1.desec.io. IN CDS ...`

  No automation so far.
- Hackathon plan: Automatically generate these records, either via
  - period cronjob, or
  - dynamic synthesis (by nameserver when queried)

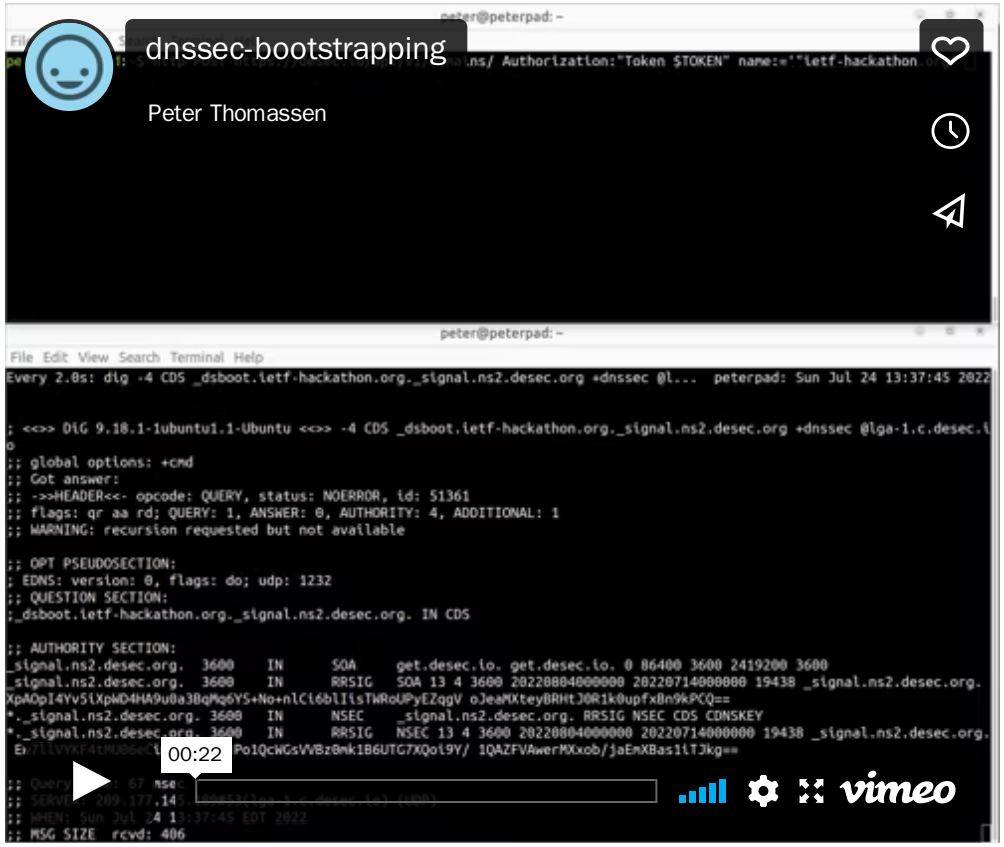
What got done

- Agreement: Expose only minimal configuration to admin
  - Tagging a zone as "bootstrapping zone" enables synthesis for all managed zones
- Code (deployed):
  - deployed:
    - saltant.net: cronjob (catalog zone → bootstrap zone) (Gitlab repo)
    - at deSEC: PowerDNS record synthesis (deSEC PR #46)
  - in the works:
    - Knot DNS module
- Techniques:
  - cronjob: Python script
  - PowerDNS: LUA records
  - Knot DNS: native C module

What we learned

- Pretty straightforward, plan worked overall
- Learned some things about LUA – good to have an expert at the table :-)
- Unexpected insight: bootstrap zones also have 2 NS records
  → need to have them on two secondaries
  - e.g. `_signal.ns1.desec.io` is hosted on ns1 *and* ns2
- Protocol seems workable in practice

Video demo


dnssec-bootstrapping
Peter Thomassen
peter@peterpad: ~
File Edit View Search Terminal Help
Every 2.8s: dig -4 CDS _dsboot.ietf-hackathon.org._signal.ns2.desec.org +dnssec @l... peterpad: Sun Jul 24 13:37:45 2022
; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> -4 CDS _dsboot.ietf-hackathon.org._signal.ns2.desec.org +dnssec @lga-1.c.desec.io
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51361
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;_dsboot.ietf-hackathon.org._signal.ns2.desec.org. IN CDS
;; AUTHORITY SECTION:
_signal.ns2.desec.org. 3600 IN SOA get.desec.io. get.desec.io. 0 86400 3600 2419200 3600
_signal.ns2.desec.org. 3600 IN RRSIG SOA 13 4 3600 20220804000000 20220714000000 19438 _signal.ns2.desec.org.
XpAOpI4Yv5iXpWD4HA9u0a3BqMq6YS+No+nlCi6blIisTWRoUPyEZqgV oJeaMXteyBRHtJ0R1k0upfxBn9kPCQ==
*._signal.ns2.desec.org. 3600 IN NSEC _signal.ns2.desec.org. RRSIG NSEC CDS CDNSKEY
*._signal.ns2.desec.org. 3600 IN RRSIG NSEC 13 4 3600 20220804000000 20220714000000 19438 _signal.ns2.desec.org.
Po1QcHGsVVBz0mk1B6UTG7XQoi9Y/ 1QAZFVAwerMXxob/jaEmXBas1lTJkg==
;; MSG SIZE rcvd: 406
00:22
vimeo

Wrap up

Team members:

Cronjob:

- John O'Brien

PowerDNS synthesis:

- Jerry Lundström
- Nils Wisiol

Knot DNS synthesis:

- Peter Thomassen

First timers @ IETF/Hackathon:

- John O'Brien
- Nils Wisiol