DNSSEC Bootstrapping

RIPE 86 Hackathon
Rotterdam, May 2023

Wat?

- Implement DNS operator side of Authenticated DNSSEC Bootstrapping, https://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-bootstrapping/

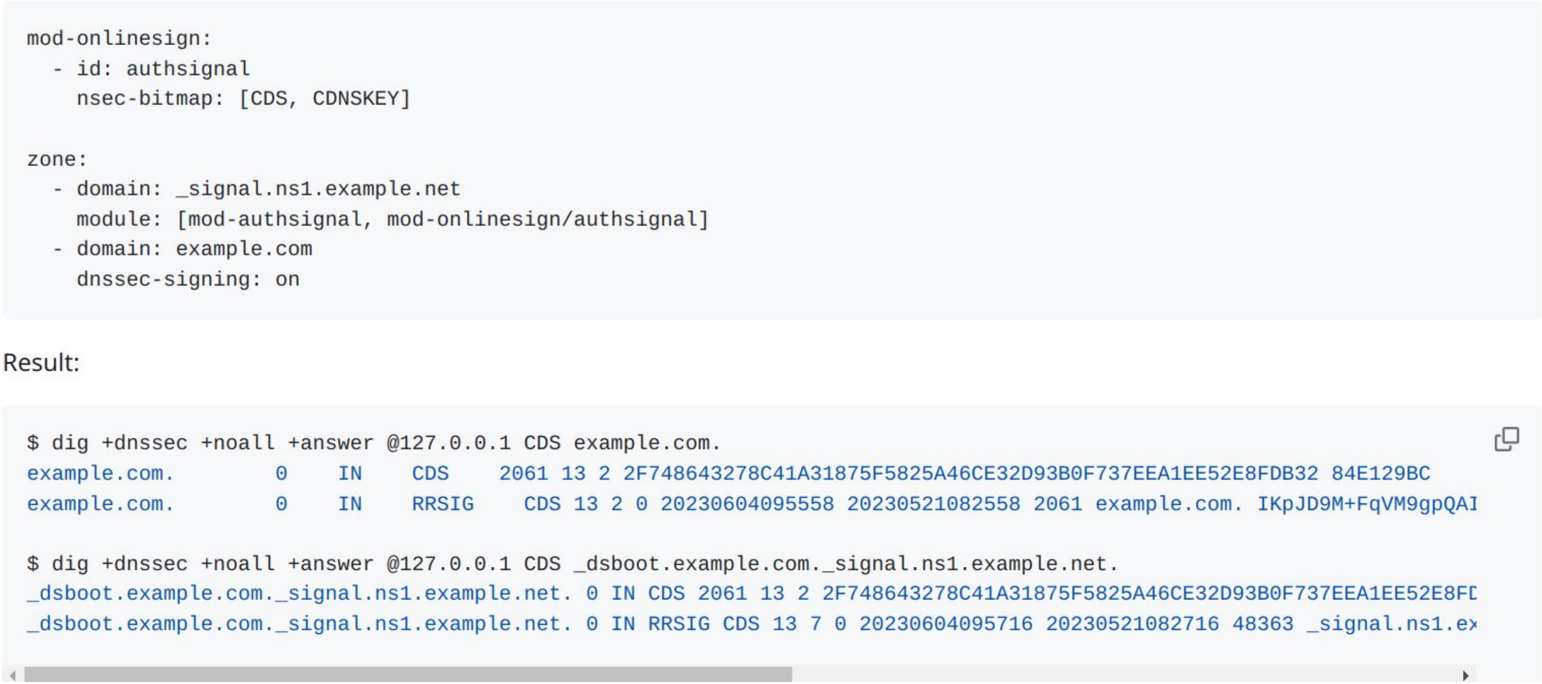
- So, **what?**
  - Given an NS hostname `$ns` and CDS/CDNSKEY records or a zone `$zone`, write code to serve a copy of those C* records under `_dsboot.$zone._signal.$ns`
  - … and sign the response properly

- And **why?**
  - Support in open source nameservers helps automatic deployment of DNSSEC

- Results: https://github.com/DNS-Hackathon-2023/DNSSEC-Bootstrapping

How? – We looked at ...

Knot DNS: new module “authsignal”



```
mod-onlinesign:
  - id: authsignal
    nsec-bitmap: [CDS, CDNSKEY]

zone:
  - domain: _signal.ns1.example.net
    module: [mod-authsignal, mod-onlinesign/authsignal]
  - domain: example.com
    dnssec-signing: on
```

Result:

```
$ dig +dnssec +noall +answer @127.0.0.1 CDS example.com.
example.com.        0    IN    CDS    2061 13 2 2F748643278C41A31875F5825A46CE32D93B0F737EEA1EE52E8FDB32 84E129BC
example.com.        0    IN    RRSIG    CDS 13 2 0 20230604095558 20230521082558 2061 example.com. IKpJD9M+FqVM9gpQAI

$ dig +dnssec +noall +answer @127.0.0.1 CDS _dsboot.example.com._signal.ns1.example.net.
_dsboot.example.com._signal.ns1.example.net. 0 IN CDS 2061 13 2 2F748643278C41A31875F5825A46CE32D93B0F737EEA1EE52E8FD
_dsboot.example.com._signal.ns1.example.net. 0 IN RRSIG CDS 13 7 0 20230604095716 20230521082716 48363 _signal.ns1.ex
```

How? – We looked at ...

BIND + Python

- Finding: dynamic synthesis
  not possible
  → prepare static signal zone

- Wrote Python code to do that
  - https://github.com/DNS-Hackathon-2023/DNSSEC-Bootstrapping/tree/main/bootstrap-bind-python

```
named-checkconf -l \   # gives all zones
  | grep -E ' (primary|secondary|master|slave|mirror)$' \
  | awk '{print $1}' \
  | python3 main.py /var/cache/bind/  # output: see slide 3 ✓
```

How? – We looked at ...

BIND + nsupdate

- Manually used nsupdate to add CDS & CDNSKEY records under _signal
- Auto-provisioning script PoC in repo ./init_bind_zone.sh
- Populates submission of _signal subdomain with CDS & CDNSKEY records to be reviewed or triggered by provider
- Work in Progress ...

Who

Adam Burns

Vincent Jumpertz

Rudi Kraus

Joeri de Ruiter

Peter Thomassen

What’s next?

- Clean up / document / upstream Knot DNS module code
- Clean up / document BIND-related code
- perhaps look at native implementation for PowerDNS?