DNSSEC Resolver Operator Recommendations

draft-mglt-dnsop-dnssec-validator-requirements

Migault - Lewis - York

Motivations

The trust in DNSSEC validation relies:

- Signature Validation: binding a RRSIG and DNSKEY RR
- Trust: the owner of the private associated DNSKEY is the legitimate owner of the signed RR.
    - Trust Anchor: the starting DNSKEY
    - chain of trust:multiple DNSKEYs recursively validated

Note that DNSKEYs are updated over time

Threat model for a DRO:

- a malicious DNSKEY RR has been introduced

Operational recommendations aim at:

- encourage DRO to enable DNSSEC validation
- provide DRO sufficient trust on DNSSEC validation accuracy

Recommendations fall into the following categories:

- Provisioning
- Monitoring
- Management
- Clarify the scope of its responsibility

DNSSEC Validator Description

```
+-------------+  +---------------+
|             |  |               |
| Time Source |  | Cryptographic |
|             |  |   Libraries   |
|             |  |               |
+-------------+  +---------------+
       |                 |
       v                 v
+--------------------------------+   +---------------+*
|                                |   |               |
|                                |<--| Trust Anchor  |
|     DNSSEC Validation Engine   |   |   Manager &   |
|                                |-->|   Storage     |
|                                |   |               |
+--------------------------------+   +---------------+
      ^ |               ^                   |
      | v               |                   |
+-------------+* +---------------+          |
|             |  |               |          |
| DNS Caches  |  | DNS Messages  |<---------+
|             |  |               |
+-------------+  +---------------+
```

DRO operations

Main intent for the recommendations are:

- minimize the possible DRO intervention. DRO should not:
    - intrument the resolver, instead let DNSSEC go.
    - require DNSSEC expert to enable DNSSEC validation
- automated operations to minimize operational errors
- focus on configuration prevention / early detection
- clarify the scope of their responsibility

Recommendations go into the following categories:

- start-up
- run time
- on-demand
    - close monitoring
    - intervention

Time deviation

START-UP REC:

- DRO MUST provide means to update the time without relying on DNSSEC when the DNSSEC validator is started. The resolver MUST NOT start if the time synchronization does not succeed at start time.

RUN TIME REC:

- While operating, DRO MUST closely monitor time derivations of the resolvers and maintain the time synchronized.

ON DEMAND REC:

- A DRO SHOULD be able to check and synchronize, on demand, the time of the system of its resolver.

TA

positive TA:

- DNSKEY (DS) /domain name association the DRO trusts

negative TA (NTA):

- a domain name the DRO disable DNSSEC validation

TA and NTA are hosted in a TA store

TA management includes:

1. TA configuration:

- DRO should be bale to define TAs/NTAs
- Ensure DNSSEC resolver start with appropriated TAs

2. TA update:

- Ensure DNSSEC resolvers appropriately roll the TAs.

3. TA reporting:

- Ensures authoritative servers is aware of the DNSKEYs in use

TA configuration

TA get updated over time

- prevent to start DNSSEC resolver with deprecated DNSKEY

The configuration of TAs, NTA is a two step process:

- *TA trust model* defines which domain is associated a TA/NTA
- *DNSKEY/DS provisionning* provisions the TA value

The (theoretical) envisioned process is:

- a) DRO defines domain names for TA and NTA (trust model)
- b) TA are retrieved/checked
- c) Generation of a configuration file (possibly YANG)
- d) DNSSEC resolver are configured and started
    - DNSSEC resolvers must not started without going to a)

Note

- Only the definition of the trust model is left to the DRO.
- TA are provisionned with the latest values and TA updates do not need to survive reboot

START-UP REC:

- DRO SHOULD only rely on TA associated with a bootstrapping mechanism.

START-UP REC:

- DNS resolver MUST validate the TA before starting the DNSSEC resolver, and a failure of TA validity check MUST prevent the DNSSEC resolver to be started. Validation of the TA includes coherence between out-out band values, values stored in the DNS as well as corresponding DS RRsets.

Implementation of these recommendations:

- A DNSSEC resolver software may embed TAs (e.g. root zone)
    - DRO trust model, retrieves the updated value and generates the configuration file (a), b) and c))
    - validation of the TA is performed by the software
- Other trust model requires requires to go trough step a-d.

TA update

START-UP REC:

- DRO SHOULD enable "Automated Updates to DNSSEC Trust Anchors" [RFC5011] [I-D.ietf-dnsop-rfc5011-security-considerations].

START-UP REC:

- DRO SHOULD enable "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)" [RFC8145] to provide visibility to the TA used by the resolver. The TA can be queries using a DNS KEY query. The channel MAY be protected and restricted to the DRO.

RUN TIME REC:

- A DRO SHOULD regularly run TA health checks.

Note that update only concerns the cached DNSKEY, not the TA and restarting the resolver every day could be sufficient

ON DEMAND REC:

- A DRO SHOULD be able to check the status of a TA

A failed key roll over is a bug in the resolver which needs to be updated and restarted.

ZKS/KSK

RUN TIME REC:

- To limit the risks of incoherent data in the cache, it is RECOMMENDED DRO enforce TTL policies of RRsets based on the TTL of the KSK/ZSK. RRsets TTL SHOULD NOT exceed the KSK / ZSK initial TTL value.

DNSKEY (TA, ZSK/KSK, NTA)

Automated Reporting (TA, ZSK/KSK)

RUNNING REC:

- A DRO SHOULD enable TA reporting to the authoritative server as specified in "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)" [RFC8145]

NTA

ON DEMAND REC:

- DRO SHOULD be able to handle NTA as defined in "Definition and Use of DNSSEC Negative Trust Anchors" [RFC7646].

RUN TIME REC:

- DRO SHOULD monitor the number of signature failure associated to each DNSKEY. These number are only hints and MUST NOT trigger automated insertion of NTA.

RUN TIME REC:

- A DRO MAY collect additional information associated each DNSKEY RRSets. This information may be useful to follow-up roll over when these happen and evaluate when a key roll over is not performed appropriately on the resolver side or on the authoritative server.

Interactions with cached RRSets

ON DEMAND REC:

- A DRO MUST be able to flush the cached data associated to a DNSKEY

Crypto deprecation

RUN TIME REC:

- A DNSSEC validator operator SHOULD regularly request and monitor the signature scheme supported by an authoritative server.

Invalid Reporting Recommendations

RUN TIME REC:

- DRO SHOULD monitor and report the unavailability of the DNSSEC service.

RUN TIME REC:

- DRO SHOULD monitor and report an invalid DNSSEC validation.

Next steps

- Internet Draft: https://tools.ietf.org/html/draft-mglt-dnsop-dnssec-validator-requirements-07
- The authors welcome feedback.
- Working Group adoption ?

Thanks!