DNSSEC Resolver Operator Recommendations

Migault - Lewis - York

Motivations

The trust in DNSSEC validation relies:

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

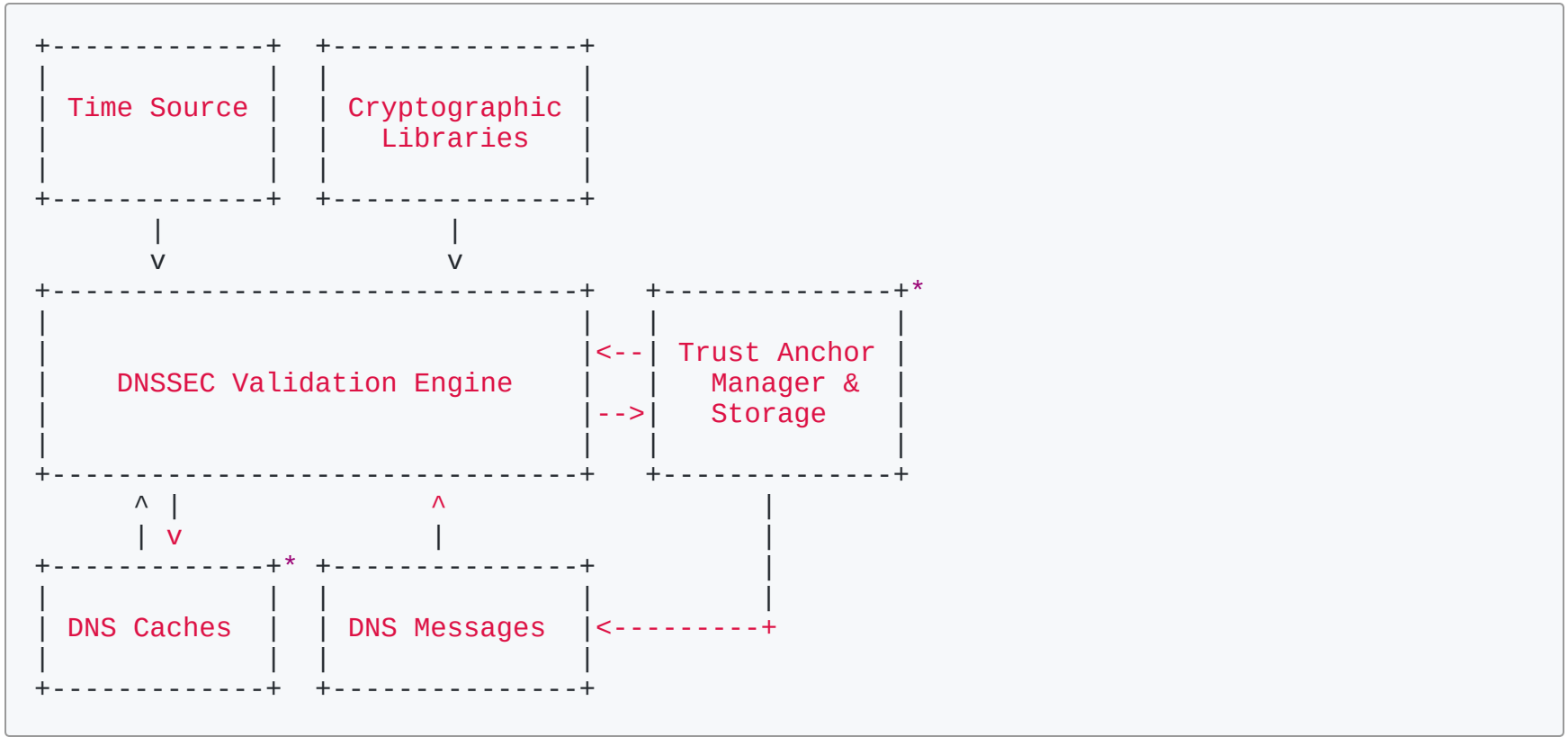
Note that DNSKEYs are updated over time

Threat model for a DRO: a malicious DNSKEY RR has been introduced

We aim at providing operational recommendations for DRO to implement sufficient trust that makes DNSSEC validation output accurate

- Provisioning
- Monitoring
- Management

DNSSEC Validator Description



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 health check
- running health check
- on-demand check/operation
    - close monitoring
    - intervention

Time deviation

start-up recommendation:

- time needs to be checked upon starting a DNSSEC resolver

running recommendation:

- regularly check time deviation

on-demand recommendation:

- DRO should be able to check time used by the DNSSEC resolver at any time

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
- b) TA are retrieved/checked
- c) resolver configuration file is generated (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 ot need to survive reboot

start-up recommendation:

- TA should have bootstrapping mechanisms (a la RFC7958)
- TA must be validated when the DNSSEC resolver is started

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

running recommendations:

- DRO must update their TA using automated update (RFC5011, I-D.ietf-dnsop-rfc5011-sec). Manual update is not permit.
- DRO must regularly compare resolvers's used TA (RFC8145) with bootstrapped TA

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

on-demand recommendations:

- A DRO must be able to retrieve TA used by resolver with associated status.

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

Automated reporting

running recommendation:

- DRO must report their DNSKEY (RFC8145) to

NTA

running recommendations:

- DRO should monitor signature failure as an hint

on-demand recommendation:

- DRO must be able to insert NTA
- DRO must be able to manage NTA as described in RFC7646

start-up recommendation:

- DRO must be able to add NTA

Interaction with the cache

on-demand recommendation:

- a DRO must be able to flush the cached data associated to a TA

KSK/ZSK (non TA)

running recommendations:

- DRO enforce TTL policies of RRsets based on the initial TTL of the KSK/ZSK
- DRO should report DNSKEY (RFC8145) to the authoritative server
- DRO should monitor validation failure for each DNSKEY

Crypto deprecation

running recommendation:

- DRO should monitor signature scheme

Next steps

- Internet Draft: https://tools.ietf.org/html/draft-mglt-dnsop-dnssec-validator-requirements-07
- The authors welcome feedback.
- Discussion may also occur within IETF DNS Operations (DNSOP) Working Group. dnsop@ietf.org
- Please help us make this a solid set of recommendations for DNS resolver operators.

Thanks!