Overview of DNSSEC Trust Anchors Repositories (TAR)

Ólafur Guðmundsson
Steve Crocker
Shinkuro, Inc.
ogud@shinkuro.com
steve@shinkuro.com

What is a Trust Anchor Repository?

- Background paper: http://www.dnssec-deployment.org/tar/tarpaper.pdf
- A collection of Trust Anchors from more than one domain that is being made “available”
- Why is TAR needed ?
  - Not all parents are signed
  - Parent publishes DS with digest that is not universally supported
  - Many others

Open TAR issues

- Disagreement on what a TAR is
- Differing opinions on what TAR’s can list
- Limited experience

- No guidance to TAR operators or users
- This talk is aimed at starting a discussion on BCP for TAR operation and use

TAR admission

Each TAR should have a policy on how TA for a NEW domain is added:

- Registration
  - Simple submission, via email, http, or DNS
  - Proof of possession tests
- Scanning/discovery
- Third party vouching (X.509 cert, PGP signatures, members submit…)
- Aggregation of multiple TAR’s

Accept TA’s even if parent is signed?

TAR maintenance

Each TAR should have a clear policy on how it maintains its contents

- SEP bit rule
    - Should Keys without SEP bit be listed as TA’s in a TAR?
- RFC5011 support
    - Monitoring frequency
    - Honor Revoke bit → delete key as soon as it is seen and validated
- Registrant notifies TAR of update
    - Same policy as new key or
    - TAR checks DNS and pulls in new TA
    - Should TAR still scan to detect changes ?
        - What to do if changes are detected ?

Deletion of TA in TAR

This is one of the sticky policies.

- When domain goes insecure or disappears
- When registrant requests ?
  - What if there is no relationship ?
- What if TA abruptly changes?

- When does a TAR stop listing a TA with a signed parent?
  - Not all domains in TAR may have DS in parent
  - Clients need time to learn the parent’s TA
  - What if TAR is using different digest algorithm than the parent?

TAR access

- Technical:
  - DNS query, DNS zone transfer, rsync file, DB lookup, email, etc.
- Policy:
  - Who can access the TAR?
    - Subscription policy
      - Fee charged ?
        - » Who pays fee, registrant or user
- Definition:
  - DLV is one type of a TAR access.

TAR influence on zone operations

- Publish SEP bit on TA’s
  - TAR’s should ignore all keys w/o SEP bit
- RFC5011/Timers rollover procedure should be used at all times.
- Monitor known TAR’s for inclusion and correctness
  - Hard to tell where all the TAR are or access contents
    - Think spam black lists

Example: ITAR (IANA Interim TAR)

- ITAR web site https://itar.iana.org/
- Admission:
  - Only TLD's can submit trust anchors
- Access:
  - Xml file containing DS records that would appear in a signed root zone, via http, ftp, (rsync failed for me April 29'th 2009 and today)
    - Tool provided to convert to trusted-keys block for Bind trust-anchors block for Unbound.
  - DNS "presentation file format" file
  - Files are PGP signed, and file digests are published.
- Usage:
  - Add to Validators configuration file, no code changes
- Updates/deletions:
  - OWNER (i.e. TLD) submits to IANA

TAR examples: ISC DLV

- ISC DLV site https://dlv.isc.org/
- Admission: (hybrid)
  - Registration with proof of access to key
    - Registration via web form, challenge sent via email
  - Includes ITAR contents
- Access:
    - DNS queries for "<name>.dlv.isc.org" type DLV
      - Requires special code in validators to look up the DLV RR and associate with the name being validated.
      - Anyone can access
- Updates/deletions:
    - Registrant, soon RFC5011

IKS-Jena TAR

- https://www.iks-jena.de/leistungen/dnssec.php
- Admission: (hybrid)
  - Scanning of TLD’s and reverse tree looking for DNSKEY RR
    - Has access to some TLD zone files
  - Open registration
- Access:
  - http, DLV: dnssec.iks-jena.de
- Updates/Deletes:
  - RFC5011

“To be or not to be” listed in a TAR

- Rathole?
- Can zone owner realistically control what someone puts in their TAR?
  - DNS data is public information.
  - Add signaling
    - Is SEP bit the way to go?

TAR or DNS on top?

- Open issue: Should validators trust verified answers from DNS when it contradicts contents of TAR or configuration?
  - Example: parent is signed and has signed delegation to the name.

Questions?