DNS operator transfers with DNSSEC

Olafur Gudmundsson

Andrew Sullivan

What is the problem?

- We are only talking about transferring DNS service, no other services.
- We wanted to describe to a domain name registrar how to transfer a DNSSEC signed domain with no outage !!
  - We failed
  - In every case there was a possible failure situation
- Go back to drawing board try to figure out a process where the goal will be satisfied.

Notation

- O = observer i.e. DNS resolver
- L = loosing DNS operator
- G = gaining DNS operator
- P = Parent or Registry
- Nl = NS set from L (before transfer)
- Ng = NS set from G (after transfer)
- Lk, Lz, = Ksk and Zsk for L
- Gk, Gz = Ksk and Zsk for G
- Kl = DNSKEY set from L
- Kg = DNSKEY set from G

DNS transfer general case

L	Nl	Nl	Nl	
P	Nl	Nl	Ng	Ng
G		Ng	Ng	Ng
O	Nl	Nl	Nl or Ng	Ng
	Before	Xfer req	Right after Xfer	Final

- Some resolvers are sticky as where to ask for information on the zone.
  - Caches that do TTL stretching and ask zone frequently enough for NS set never to time out.
- Unless L stops serving zone resolvers may take **real long time** to discover new set of nameservers.
  - How long is sticky → one TTL after L stops serving is when we can be sure

R3: Registrar, Registrant, Registry complications

- ICANN current transfer policy allows for uncooperative participants.
- Timing of actions can not be predicted.
  - L can accept, ignore or contest transfer request.
  - No requirement that L stop serving up zone after transfer
- G can not send Ng to L via registry
  - G can try to change contents of registry to Ng before transfer via owners account

DNSSEC transfers

- Assumptions:
  - Domain is signed, by L
    - L has both KSK and ZSK private keys and will not share them with G.
  - G will sign the zone with different set of keys.
    - G will list L's keys
  - L will be minimally cooperative
- Complication:
  - for some time validators may have data from the zone some signed by L and some signed by G due to TTL's.
    - We do not want validation failures

DNSSEC validation error possibilities

- Before switch:
  - Parent must list DS for both L and G's or validation will fail.
    - New DS must be given time to propagate before NS is changed.
- When parent switches referral from L to G caches:
  - Cache ignorant of the zone is not affected
  - Cache has Kl and learns Ng.
    - Verification may fail until Kl times out

Solution: additional steps

- Credit: Antoin Verschuren proposed this general approach
- Step 1:
  - L and G include both of sets of ZSK keys in their DNSKEY RRset.
    - Kl (L DNSKEY) = Lk, Lz, Gz
    - Kg (G DNSKEY) = Gk, Lz, Gz
- Step 2:
  - Parent adds Gk to DS, listing both Lk and Gk
- Step 3: (actual transfer) (wait at least 1 DS TTL)
  - Parent updates NS from Nl to Ng

Complications

- "Requires" L to cooperate in the transfer
  - If both L and G are under contract with owner → not a problem.
- Registry is natural conduit for Gz to L
  - Publication of Gz key by L is acceptance of transfer
  - EPP protocol needs to be updated for this to happen,
    - L needs to keep serving the zone for a while after agreeing to transfer
    - Registry accepts Gk from G and after transfer request is accepted adds that to DS.
    - Additional data in transfer request: Gz.
    - L needs to stop serving the zone when told by the registry.
  - Agreements specifying transfers need to be updated.
    - → Tools and processes need to be updated.

Discussion