Secure zones during transfers

Roy Arends

Nominet UK

Transitions

- Zone moves from registrant to registrant
- Zone moves from operator to operator
- Zone moves from registrar to registrar
- Zone moves from registry to registry
- DNSKEY update
- HSM upgrade
- DNSSEC Signing Software update

DNSKEY Rollover

- All of these require a DNSKEY rollover
- Some have additional requirements
- Main requirement:
  - Validating resolvers must see the zone as signed during transition
- Validating resolvers also cache DNS information

DNSKEY rollover

- A signature identifies the KEY needed to validate
- When there are two zones by different entities, there are two keys as well, one for each zones.
- Assume KEY and SIG “OLD” and “NEW”
- Key OLD can’t validate sig NEW
- Key NEW can’t validate sig OLD

DNSKEY Rollover

- Once keys and signatures are cached, the resolver will not refresh them until the DNS TTL for these records have expired.
- DNSSEC Lockout:
  - OLD key/NEW sig are cached or
  - NEW key/OLD sig are cached
  - Can't validate
  - Won't refresh

Requirement

Requirement

AVOID LOCKOUT

Roy's Simple Registry Transition

- Assumptions:
  - Gaining registry has full zone file copy, including signatures (but no access to old private keys)
  - Signatures are valid for some time in the future

Roy's Simple Registry Transition

1. Add 'EBERO' DS records next to 'OLD' DS records to parent before transition.
   - This allows validators to follow an alternative chain of trust when it comes available
   - Takes 'DS TTL' seconds (currently 1 day)

Roy's Simple Registry Transition

2. Augment the zone by:
   - Replace old KSK with EBERO KSK
   - Add ZSK to the zone (keep old ZSK)
   - Sign the DNSKEY RRSet with new KSK
     - Replace the 'OLD' DNSKEY signatures
   - Sign zone with new ZSK
     - Keep the 'OLD' signatures

Roy's Simple Registry Transition

3. Re-delegate zone to new servers

- after (parent NS TTL) seconds, all validators migrated to the new zone on the new server
- What remains is the last steps of a regular DNSKEY rollover
  - Retire the old ZSK
  - Retire the old ZSK Signatures

LOCKOUT scenario 1

- Old Signatures and New Keys
- Old signatures cached
- Old DNSKEY still available in new zone

- All rejoice, no Lockout

LOCKOUT scenario 2

- NEW Signatures and Old Keys
- OLD Keys cached
- OLD Signatures available in new zone
  - (New signatures can only come from the new zone, where the old signatures are available as well)
- All rejoice, no Lockout

What just happened?

- We have transitioned a zone while maintaining DNSSEC integrity.
- Timing is _critical_ as old signatures have limited shelf live.

Why does this work?

- This is essentially “Double DS Method”
  - draft-ietf-dnsop-dnssec-key-timing-03
  - Section-3.3.2

- In this scenario, no cooperation needed from the old DNSKEYs