dry-run DNSSEC

draft-yorgos-dnsop-dry-run-dnssec

Yorgos Thessalonikefs, Willem Toorop, Roy Arends

IETF 122

Recap

- Inspired by DNS Error Reporting (now RFC 9567)
- Soft fail DNSSEC errors and report back (think DMARC)

Disclaimer

- The current version (-03) is wrong!
- Not really, made simpler, dry-run only for insecure zones
- More on that later

Use case - going secure

- Insecure zone is signed and published
- A dry-run DS record (dry-run algorithm) is published in the parent
- Non-aware resolvers treat as insecure
- The rest generate DNS Error Report on validation failure; fallback to insecure
- If validation succeeds return AD bit (opportunistic security)
- ~~If~~ *When* everything is ok, turn-key action: update DS

NOERROR report

- Absence of failure reports needs to translate to a positive message
  - Is there anybody out there?
- If no DNSSEC failure encountered, the resolver generates a NOERROR report for the zone apex
  - This is for the resolver to cache the noerror generation; no need to spam the reporting agent with those
  - FIXME: problematic with forwarders

Signaling

- Explicit DS Digest Type Algorithm for dry-run
- Intention to burn-a-bit for dry-run counterpart
- Currently on the draft only counterpart for SHA256 to get things rolling

Provisioning

- Either parent accepts DS
- Or parent needs to get the dry-run intent
  - Peek at the DS, UI option, other
- CDS works
  - CDNSKEY needs accompanying CDS
- (Burn-a-specific-bit makes parsing easier)

Extra: end-to-end testing

- Clients can opt-in (with new EDNS0) to receive dry-run DNSSEC errors (if any)
- Easier debugging from the client side
- Useful to test how an application will behave in case of errors

What was left behind

- Theoretically can work on already DNSSEC zones
- But not-trivial, since signaling is on DS and there is only one DNSKEY set; can only work for different algorithms
- Left out to make draft simpler
- Whatever comes out of dd wg could point to different DNSKEY sets
- If dry-run proves useful can be augmented for DNSSEC experimentation and testing key rollovers in the deleg era

Security caveat

- Data integrity dropped on the floor
- In case of DNSSEC errors (or attacks) the resolver fallbacks to insecure
  - *Feature not a bug*
- Warning that dry-run DNSSEC is a temporary intermediate step of a zone going secure

Why do all this?

- Confident testing for signing
- In production, the real thing
- No fires to put out in the middle of the night
  - Friends don’t let friends ask other friends to clear their caches
- Turn key solution to go live (change the DS, don’t touch the proven signed zone data)
- …
- DNSSEC adoption?

When life gives you DNSSEC failures…

Gunshow, by KC Green

When life gives you DNSSEC failures…

dry-run

dry-run with end-to-end testing

Gunshow, by KC Green

u/GameNCode on reddit

u/leolambertini on reddit

dry-run DNSSEC

Comments / Questions / Adoption ?

Appendix

- Favourite color:definitely blue
- Capital of Assyria:
  - Assur (c. 2025–1233 BC)
  - Kar-Tukulti-Ninurta (c. 1233–1207 BC)
  - Assur (c. 1207–879 BC)
  - Nimrud (879–706 BC)
  - Dur-Sharrukin (706–705 BC)
  - Nineveh (705–612 BC)
  - Harran (612–609 BC)
- Air-speed velocity of an unladen european swallow: roughly 11 meters per second, or 24 miles an hour