Consistency for CDS/CDNSKEY (and CSYNC) is Mandatory

draft-thomassen-dnsop-cds-consistency

IETF 116 – DNSOP WG
March 30, 2023

Peter Thomassen (deSEC, Secure Systems Engineering)

Security Risks in Automatic Delegation/Trust Maintenance

- **CDS/CDNSKEY** spec says nothing about how parent should poll (RFC 7344)
  - Parents likely use standard resolution for retrieving CDS/CDNSKEY records from child
  - Used for **automatic DS management** (key rollovers, bootstrapping) → potential **security impact**
- **CSYNC** spec advocates limiting queries to just one auth (RFC 7477 Sec. 3.1)
  - Even suggests asking all (+ compare serial) **for freshness, not consistency** (Section 4.2)
  - Used for **delegation updates** (hostnames/glue, provider change) → potential **security impact**
- **Asking a single nameserver does not ensure consistency** across auths
  - When there are several operators, this **can go seriously wrong** (even with domain lock!)
  - Example failure modes: **(1) multi-homing, (2) provider change** → backup slides

❗ **Each nameserver operator is a single point of failure / can break delegations** ❗

New Failure Mode: **Lame Delegation Hijacking**

- EPP has a quirk that sometimes prevents removal of expired NS names
  - Registering expired name equivalent to on-wire attacker → **DNSSEC offers integrity protection**
  - **512K domains exposed** to this risk and **163K taken over** between 2011 and 2020 (https://dl.acm.org/doi/10.1145/3487552.3487816)

- C* records enable new attack vector: **Full domain take-over**
  - Stage 1
    - Hijacker **publishes their own keys** via CDS/CDNSKEY
    - When processed by parent, responses from **remaining legitimate auths become bogus** → **broken** (availability)
  - Stage 2
    - Hijacker **publishes NS and CSYNC** in child (all NS under their control)
    - When processed by parent, **remaining legitimate auths removed** from delegation → **broken** (integrity)

→ **Attacker now positioned as only party providing auth service for the victim domain**

Updates since last IETF

- Basics unchanged: **process C* RRsets only when consistent across auths**
  - Disregard unresponsive servers
- Added OPTIONAL retry mechanism for resolving inconsistencies
  - Exponential backoff
- Editorial changes
  - Expanded motivation section to include new failure mode (lame delegation hijacking)
- Question: CDS updates MUST NOT break validation. **How about CSYNC?**
- Next steps?

Backup

Failure: **Multi-homing**

- Expectation: multi-homing guarantees provider independence!

- DS breakage (multi-signer):
  - Provider forgets to include other providers' keys in CDS/CDNSKEY (e.g. after key roll)
  - When processed by parent, **other providers' keys removed** from chain of trust
    → **broken**

- NS breakage:
  - Provider publishes *incomplete* NS record set + CSYNC (e.g. after changing their hostnames)
  - When processed by parent, **other providers removed** from delegation
    → **broken**

Another Failure: **Provider Change**

- Unless going insecure, workflow requires **brief multi-signer period**:
  - Providers import each other's keys into their DNSKEY/CDS/CDNSKEY RRsets
  - DS update is triggered (via changed CDS/CDNSKEY records at old provider)
  - Once DS is updated: add new provider to NS record set (e.g. by old provider via CSYNC)
    → **multi-signer mode fully operational** at this point
  - … reverse steps to offboard old provider

- Complication: New provider does not actually import any keys
  - (Perhaps unaware of multi-signer and its intricacies)
  - Some "DNSSEC out-of-the-box" offers just **sign with fresh key pair + publish CDS/CDNSKEY**
  - From here, we're headed for **"multi-homing failure"**
    → **DS breakage** (other provider's keys removed)
    → **NS breakage** (other provider's nameservers removed)