Scalability of Scanning

… of CDS/CDNSKEY records

ICANN 77 – DNSSEC Workshop
June 12, 2023

Peter Thomassen
peter.thomassen@securesystems.de

Scalability of CDS/CDNSKEY scanning

Architecture	Scanning not optimal: Lots of fishing; very few fish
RFCs deployment	(RFCs 7344, 8078) and deployment CSYNC (RFC 7477)
Survey	5 responses among Ry/Rr supporting (or working on) CDS scanning
Other	Numbers gathered from large-scale DNS measurements

Survey Results

	Number Time	Concerns/Comments	Comments
Response 1	2.5M 6 hrs	• Configuration tuning necessary (file descriptors) • Some targets don't support pipelining • can go much higher	• One server per location • Cross-location consistency enforced • Have published SLA
Response 2	400K 5 hrs	Perhaps .com, but maybe let Rr do it?	• One server • Going to scan other TLDs (14M) • Final frequency not decided
Response 3	?? ??	none	• One machine per TLD • No scaling issues • SLA likely "delay ≤ 1 day" • Open to implement NOTIFY
Response 4	8K ??		• One server • No SLA
Response 5	20M ??	Ry rate-limit .com extremely feasible	• One VM • Email customer on update • Not planning to implement NOTIFY

Survey Summary

- O(10M)–O(100M) daily scanning on a single VM
- Higher numbers can be achieved
- No concerns about load
- Mixed openness for NOTIFY

- Change reporting to registrant in at least one case
- One participant proposed that for very large TLDs, Rr should scan
- In some cases scanning is subject to TLD rate limits

Numbers from (unrelated) DNS Measurement Experiments

– – –

- For DNSSEC and DANE Deployment Statistics
  Viktor Dukhovni scans O(20M) domains daily
  - Query count ~95M (DS, DNSKEY, MX, A/AAAA once per MX, TLSA if MX is signed, …)
  - Takes about 4 hours on 32-core machine
  - Scaling up to non-stop querying would allow ~500M queries per day on single machine

- For OpenINTEL
  Roland van Rijswijk-Deij et al. scans about 5B queries daily
  - 250M domains daily (estimated ~65% of the namespace)
  - All of the IPv4 reverse DNS (~4.3G addresses)
  - OpenStack cluster on 4 machines, with load 25–50% spread throughout the day

Interpretation

- Scanning seems feasible from a practical perspective
  - At current rate, e.g. daily
- Scaling mostly takes advantage of core CDS/CDNSKEY assumptions
  - Records are either permanent and unchanging, or only present during key rollovers
  - Comparing binary RDATA equality good enough for detecting a change (after canonicalization)
  - Doing signature validation against existing DNSKEYs doesn't need to happen much
- Main concern: **expected reaction time** (days? hours? minutes? seconds?)
  - Quick turnaround achievable via on-demand triggers (= notification from child to parent)
  - It's very clear that any expectation for "quick scanning" would be misguided
    → If you want quick updates, send a notification

Summary

- Daily scanning seems feasible
  - Some deployments; more to come
  - Rate limits impede scanning speed in some cases
- Response time is around a day
- NOTIFY would greatly reduce delay
  - Standardization is under consideration
    - (draft-thomassen-dnsop-generalized-dns-notify)
- Manual interface MUST remain
  - For quicker fixes
  - More importantly: to roll DS RRset if you lost your private key (can't sign CDS!)

Backup

Who's in Charge of Polling?

	Registar	Registry
DS Flow	DNS Operator → Registrar → Registry (no EPP backchannel needed)	DNS Operator → Registry → Registrar (requires EPP backchannel, RFC 9167)
Deployment (today)	- 1 (Domainnameshop) - 1 planned (GoDaddy, since 2020)	- 10 (9 ccTLDs + RIPE) - Several gTLDs ready (CentralNIC, CORE)
Scope	- Covers gTLD and ccTLD names	- Covers only gTLD names
Pros	- Preserves customary flow	- Adoption appears easier in Ry space - Fewer steps to DS (EPP notify is async)
Cons	- TLD query and/or EPP rate limit - Adoption difficult, many Registrars - Some even lack DS interface today - Some charge for setting DS - NOTIFY target discovery unclear	- No ccTLD coverage in Ry agreements, potentially limiting recommendation scope