Experimental Results on DNSSEC Record Delivery

Austin Hounsel [1] **Eric Rescorla** [2]
Chris Wood [3] Nick Feamster [3]

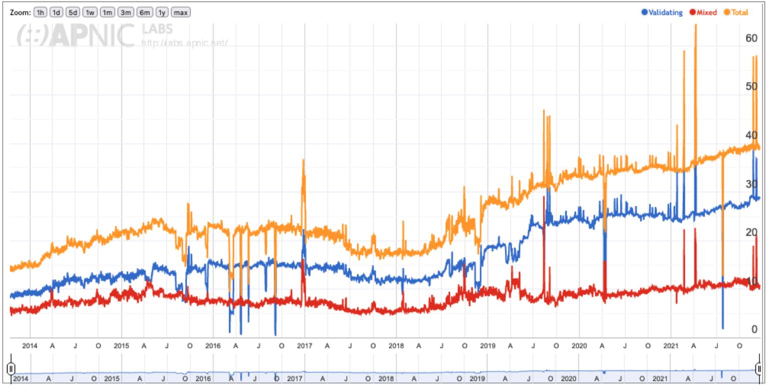
[1]Princeton University

[2]Mozilla

[3]Cloudflare

2022-07-28

Lots of DNSSEC Validation



Nearly all of this is by recursive resolvers

- No major operating system does endpoint DNSSEC validation by default
- Browsers don't do it either
- This is limiting
    - A number of DNSSEC-based mechanisms need endpoint validation (e.g., DANE)

Why don't endpoints validate?

- Concerns about performance
  - More requests may be slower
- **Concerns about breakage**
  - If DNSSEC records aren't delivered this is indistinguishable from an attack
  - Resolvers are supposed to hard-fail
  - Any significant rate of non-delivery will create unacceptable failure rates
  - Little actual data

Experimental Setup

- Set up some domains with known contents
  - Correct DNSSEC records
  - Some other less-common records
- Use Firefox as a measurement platform
  - Randomly select a sample of clients
  - Each client directly resolves the relevant records via UDP and TCP
    - Bypassing the system resolver
  - Measure the success rate

Queries

- A record via the Firefox `dns.resolve()` API
- A records with all values of DO and CD
- DNSKEY
- HTTPS SVCB record.
- SMIMEA record.
- Small (8 bytes) and large (1023 bytes) records with code points in "Expert Review" and "Private Use" ranges

Results

Query	Failure Rate
A	0.022 (0.021–0.023)
A (CD=1)	0.024 (0.023–0.024)
A (DO=1)	0.387 (0.385–0.389)
A (DO=1, CD=1)	0.388 (0.386–0.390)
DNSKEY	0.023 (0.022–0.023)
SMIMEA	0.140 (0.138–0.141)
HTTPS	0.065 (0.064–0.066)
NEWONE	0.203 (0.201–0.204)
NEWTWO	0.214 (0.212–0.216)
NEWTHREE	0.281 (0.279–0.283)
NEWFOUR	0.289 (0.287–0.291)
A (WebExt API)	0.004 (0.004–0.005)

Impact

- It's not safe to enable endpoint DNSSEC validation over Do53
  - At least not for end-user clients
  - The situation is different for servers
- Might be safe to enable over DoH/DoT
  - Public resolvers do a lot better
  - Might be the case that ADD-advertising resolvers do better
- Somewhat practical to deploy other record types
  - As long as it fails safe if they are not found
  - HTTPS looks especially good

Questions?