Unilateral DNS Probing between Recursive and Authoritative Servers

IETF 112 DNS Privacy (Nov 2021)

Joey Salazar and Daniel Kahn Gillmor

draft-dkgjsal-dprive-unilateral-probing

Why Unilateral?

What can an adopter do *without* worrying about signalling?

- Opportunistic
- Still vulnerable to active adversary
- Should not preclude a more robust approach

Raise the floor without lowering the ceiling

Should inform thinking about signalled/negotiated connections

Concerns

- Increased latency
- Excess resource consumption
- Accidental data leakage

Remember the legacy of STARTTLS in SMTP, IMAP, etc.

Authoritative Servers

- Listen with DoT on TCP port 853
- Listen with DoQ on UDP port 853

Authentication: use any X.509 certificate, ignore SNI

DoH could only be used by choosing an "expected" path. Is there a better way?

Recursive Resolvers (part 1/2)

- Probing for DoT and/or DoQ by authoritative IP address
- Similar to "happy eyeballs"
- Draft maps out internal state, and outlines how to update it

…

Recursive Resolvers (part 2/2)

…

Overall parameters governing each encrypted connection to an IP:

- `persistence`: remember success (3 days)
- `damping`: avoid retrying after failure (1 day)
- `timeout`: acceptable delay (30 seconds)

Signal Info? (part 1/2)

What would we need from a signal to do better than this?

- What authenticated encrypted transport is expected to be running?
  - DoT or DoQ or both?
- What authentication type should be used?
  - X.509 or DANE
- What name to authenticate against?
  - NS name? Something derived from the zone itself?

…

Signal Info? (part 2/2)

…

- Whether to hard fail ("STS")
  - Is there any utility in an intermediate indicator?
- How/where to signal if secure authenticated transport fails
  - This smells like TLSRPT

Interaction with Signals? (part 1/2)

Signals are likely to be bound to domains or nameserver names.

Data from probes are bound to IP addresses.

Should info from signalled connections also update probe data? If so, how?

…

Interaction with Signals? (part 2/2)

…

Probes don't send SNI. Signalled connections might send SNI? (privacy leak)

Could a signalled connection succeed where a probe fails?

Comparison with other drafts

On signalling:

- draft-ietf-dprive-unauth-to-authoritative
- draft-rescorla-dprive-adox-latest (expired)
- draft-vandijk-dprive-ds-dot-signal-and-pin (expired)

On probing:

- ?

Critique, Suggest, Contribute!

https://gitlab.com/dkg/dprive-unilateral-probing