Unilateral DNS Probing between Recursive and Authoritative Servers

IETF 113 DNS Privacy (March 2022)

Joey Salazar and Daniel Kahn Gillmor

draft-ietf-dprive-unilateral-probing

Covered in this draft

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

- Authoritative Servers: Listen with DoT/DoQ on TCP/UDP port 853
- Recursive Resolvers: Probing for DoT/DoQ by authoritative IP address

Concerns: Latency, resource consumption, data leakage

Guidance for Authoritative Servers and Recursive Resolvers

Not covered in this draft

Probing for DoH

Signalling mechanisms

Changelog

-01 to -02 (now draft-ietf-dprive-unilateral-probing-00)

- Clarify that deployment to a pool does not need to be strictly simultaneous
- Explain why authoritatives need to serve the same records regardless of SNI
- Defer to external, protocol-specific references for resource management
- Clarify that probed connections must not fail due to authentication failure

draft-dkgjsal-dprive-unilateral-probing -00 to -01

- Fallback to cleartext when encrypted transport fails.
- Reduce default `timeout` to 4s
- Clarify SNI guidance: OK for selecting server credentials, not OK for changing answers
- Document ALPN and port numbers

Current FIXMEs

- Questions regarding the Probing Policy (4.5) and encrypted transport connections
- Questions on combining Signals with Opportunistic Probing (5.1)

Comparison with other drafts

- draft-ietf-dprive-unauth-to-authoritative (superseded)
- draft-ietf-dprive-opportunistic-adotq (superseded)
- draft-pp-recursive-authoritative-opportunistic (superseded)
- draft-rescorla-dprive-adox-latest (expired)
- draft-vandijk-dprive-ds-dot-signal-and-pin (expired)

Critique, Suggest, Contribute!

- Mailing list reviews and comments
- GitHub issues and pull requests

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