Using Early Data in DNS over TLS

draft-ghedini-dprive-early-data

Alessandro Ghedini, Cloudflare

TLS 1.3 early data:

- TLS 1.3 (RFC8446) introduced 0-RTT session resumption, which allows clients to send application data in the first round-trip of the handshake.
- Can be used to send DNS over TLS queries without having to wait for the TLS handshake to complete.
- Can be useful when DoT connection might not be long-lived (e.g. mobile clients), or to avoid keeping lots of connections open (e.g. resolver->authoritative).

Caveats:

- Early data can be intercepted and replayed (in encrypted form) by on-path attackers, so only idempotent queries should be sent as early data.
- This has also implications for DDoS and privacy.

RFC8446, Appendix E.5:

> Application protocols MUST NOT use 0-RTT data without a profile that defines its use. That profile needs to identify which messages or interactions are safe to use with 0-RTT and how to handle the situation when the server rejects 0-RTT and falls back to 1-RTT.

DNS over TLS Early Data:

- Draft is mostly based on RFC8470 as many things are common between HTTP and DNS (e.g. client retry behavior).
- DNS-specific bits: forbid some "unsafe" queries (e.g. DNS Updates, Zone Transfers, ...), some security considerations.

Open issues:

- Define whitelist of allowed RR types (e.g. IANA registry) instead of a blacklist of not allowed ones.
- Add privacy considerations text.

Next steps:

- WG adoption?