Using Early Data in DNS over TLS

draft-ghedini-dprive-early-data

Alessandro Ghedini, Cloudflare

Recap:

- TLS 1.3 (RFC8446) introduced 0-RTT session resumption, which allows clients to send application data in the first round-trip of the handshake ("early data").
- 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 messages should be sent as early data.

For this reason TLS 1.3 mandates that application protocols that want to use early data have to define a policy for when it is safe to do so (see RFC8446, Appendix E.5).

Draft status:

- Originally presented at IETF 105.
- Went through some rounds of discussion on the mailing list.

Changes in draft-02:

- Only DNS messages with "Query" opcode are allowed.
- Introduced whitelist (via new IANA registry) of "safe" RR types that can be used in early data.
- Other editorial fixes suggested by reviewers.

The RR types whitelist is not complete right now, additional types can be added later on once it is decided that this is a good approach.

Open issues:

- Do we really need the RR type whitelist, or is only allowing Query messages enough? The objective is excluding non-idempotent DNS messages.
- If whitelist is to remain, other RR types need to be reviewed for addition to the list.

Next steps:

- WG adoption?