draft-hzhwm-dprive-start-tls-for-dns: DNS over TLS

A bunch of authors

IETF 92, Dallas

v.3

Protocol overview

- Privacy provided by TLS over TCP
- First do port-based:
  - Try to start TLS on a new to-be-allocated port; if so, done
- If not, do upgrade-based:
  - Send a real or dummy query on port 53 with a new EDNS0 flag, TO
  - If the client gets TO back, starts TLS
- Can be authenticated or opportunistic TLS

Design choices

- This should be a protocol drop-in for the current DNS infrastructure
- Few currently-deployed middleboxes block unassigned TCP ports, but some middleboxes (still!) block TCP/53
- Thus, SHOULD try port-based first
  - But might order the other way based on cached info or configuration
- Primary target for the WG is stub-to-resolver, so a long-lived TCP connection makes sense
- No new crypto or transports

Authenticated and opportunistic

- This spec doesn't change the current way DNS resolvers are found: either through a configured IP address, or whatever the DHCP server specifies
- Authenticated TLS for DNS can be done using IP addresses in the server cert
  - There is no expectation that these will be issued by the current web CAs, but they could be
- Opportunistic is done by the client automatically trusting the server's cert, just like it is for SMTP

Changes since IETF 91

- Added “try port-based TLS first” to existing upgrade-based TLS
- Added more about motivations throughout the document
- Documented a few more open issues
- Added Paul Hoffman as co-author

Implementation

- An implementation of upgrade-based was shown at the last IETF, and remains unchanged
- Lots of implementation experience with DNS over long-lived TCP not requiring extra round trips
  - When TCP is up, this is one packet request, one packet reply just like UDP
- Implementation experience with TCP Fast Open (RFC 7413) and TLS resumption
  - Can push all state to client; client can then resume quickly even when TCP is torn down