DNS Privacy reference material

Relevant Internet Drafts and RFCs

DPRIVE

RFC7626	**DNS Privacy Considerations**	This document describes the privacy issues associated with the use of the DNS by Internet users. It is intended to be an analysis of the present situation and does not prescribe solutions.
RFC7858	**Specification for DNS over TLS**	This document describes the use of TLS to provide privacy for DNS.
RFC7830	**The EDNS(0) Padding Option**	his document specifies the EDNS(0) 'Padding' option, which allows DNS clients and servers to pad request and response messages by a variable number of octets.
draft-ietf-dprive-dtls-and-tls-profiles	**Authentication and (D)TLS Profile for DNS-over-TLS and DNS-over-DTLS**	This document describes how a DNS client can use a domain name to authenticate a DNS server that uses Transport Layer Security (TLS) and Datagram TLS (DTLS). Additionally, it defines (D)TLS profiles for DNS clients and servers implementing DNS-over-TLS and DNS-over- DTLS
https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsodtls/	**Specification for DNS over Datagram Transport Layer Security (DTLS)**	
draft-ietf-dprive-eval	**Evaluation of Privacy for DNS Private Exchange***	This document describes methods for measuring the performance of DNS privacy mechanisms, particularly it provides methods for measuring effectiveness in the face of pervasive monitoring as defined in RFC7258.

DNSOP

RFC7766	**DNS Transport over TCP - Implementation Requirements***	This document specifies the requirement for support of TCP as a transport protocol for DNS implementations and provides guidelines towards DNS-over-TCP performance on par with that of DNS-over-UDP.
RFC7816	**DNS Query Name Minimisation to Improve Privacy**	

RFC7828	**The edns-tcp-keepalive EDNS0 Option***	This document defines an EDNS0 option ("edns-tcp-keepalive") that allows DNS clients and servers to signal their respective readiness to conduct multiple DNS transactions over individual TCP sessions.

Other

RFC5246	**The Transport Layer Security (TLS) Protocol**
RFC7525	**Recommendations for Secure Use of TLS and DTLS**
RFC7413	**TCP Fastopen**

Selection of Presentations

A short video is available demonstrating TCP connection re-use, pipelining, TCP Fast Open and DNS-over-TLS: DNS-over-TLS demo video

- **IETF 97 EDU Privacy Tutorial**
  - DNS Privacy Tutorial (Sara Dickinson, Daniel Kahn Gillmor)
- **RIPE 72**
  - DNS Privacy Public Resolver discussion (Sara Dickinson)
- **IETF 94:**
  - DNS-over-TLS draft update (D. Wessels, S. Dickinson)
- **IETF 93:**
  - Update on 5966bis and EDNS0 keepalive (Sara Dickinson)
- **DNS-OARC Fall workshop 2015:**
  - Using TLS for DNS Privacy in practice (Sara Dickinson)
- **IETF 91:**
  - DNS over TCP and TLS - draft-hzhwm-dprive-start-tls-for-dns-00 (John Heidermann, Sara Dickinson)
- **IETF 89:**
  - T-DNS: Connection-Oriented DNS to Improve Privacy and Security (Duane Wessels)
- **DNS-OARC Spring workshop 2014**:
  - T-DNS: Connection-Oriented DNS to Improve Privacy and Security (John Heidemann)
  - getdns-api implementation (Willen Toorop)

getdns API

- **getdns API homepage** (http://getdnsapi.net/about.html)
- **Description of the getdns API** (https://getdnsapi.net/spec.html)

Technical reports

- **T-DNS: Connection-Oriented DNS to Improve Privacy and Security** (http://www.isi.edu/publications/trpublic/files/tr-693.pdf)
- http://googlecode.blogspot.co.uk/2012/01/lets-make-tcp-faster.html

Example code

- **ANT project software for DNS analysis and privacy** http://isi.edu/ant/software/