DNS Privacy - The Solutions

This site is mainly focussed on following the development and deployment of DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) as the leading solutions for DNS Privacy because they are the only protocols currently standardized by the IETF.

Some history and background on other alternatives are outlined below and we intend to follow other solutions as they evolve.

- DNS-over-TLS (DoT)
- DNS-over-HTTP (DoH)
- DNS-over-DTLS
- DNSCrypt
- DNS-over-HTTPS (proxied)
- DNS-over-QUIC
- DNSCurve

DNS-over-TLS (DoT)

RFC7858 specified DNS-over-TLS as a Standards Track protocol in May 2016 with a port assignment of 853 from IANA. There is active work in this area.

There are now multiple implementations (including Stubby a local DNS Privacy stub resolver) and a number of experimental and public servers deployed.

DNS-over-HTTP (DoH)

RFC8484 specifies DNS-over-HTTPS as a Standards Track protocol on October 2018.

There are several implementations (including Firefox) and deployments. Note that with DoH it is possible to intermingle DNS and HTTP traffic on the same port 443 connection and make blocking of encrypted DNS harder. It should be noted that this RFC addresses almost purely protocol issues, there is no dynamic discovery mechanism for DoH specified yet so it cannot be done opportunistically (it must be configured).

DNS-over-DTLS

RFC8094 specified DNS-over-DTLS as an Experimental Standard in Feb 2017. To our knowledge that are no implementations of DNS-over-DTLS planned or in progress.

One issue with DNS-over-DTLS is that it must still truncate DNS responses if the response size it too large (just as UDP does) and so it cannot be a standalone solution for privacy without a fallback mechanism (such as DNS-over-TLS) also being available.

DNSCrypt

DNSCrypt is a method of authenticating communications between a DNS client and a DNS resolver that has been around since 2011.

- It prevents DNS spoofing.
- It uses cryptographic signatures to verify that responses originate from the chosen DNS resolver and haven't been tampered with (the messages are still sent over UDP).
- As a side effect it provides increased privacy because the DNS message content is encrypted.
- It is an open specification but it has **not** been standardized by the IETF.
- There are multiple implementations and a set of DNSCrypt servers available.
- OpenDNS offers DNSCrypt

Also check out an in depth comparison from Tenta.

DNS-over-HTTPS (proxied)

There are implementations available (e.g. from BII) of proxies that will tunnel DNS-over-HTTPS.

Google offers a proprietary DNS-over-HTTPS service using a JSON format for DNS queries.

A new working group was formed in Sept 2017 by the IETF: DNS-over-HTTPS (DOH)

DNS-over-QUIC

A draft was submitted in April 2017 to the IETF QUIC Working group on DNS-over-QUIC

DNSCurve

DNSCurve was developed in 2010 with encrypting the resolver to authoritative communications in mind. It was not standardized by the IETF.