DNS Privacy - The Problem

Why is DNS a privacy concern?

> The DNS is one of the most significant leaks of data about an individuals activity on the Internet.

Some of the issues in simple terms:

- Almost every activity on the Internet starts with a DNS query (and often several). A key function of the DNS is to map human readable names (e.g. example.com) to IP addresses that computers need in order to connect to each other.
- Those queries can reveal not only what websites an individual visits but also meta data about other services such as the domains of email contacts or chat services.
- Whilst the data in the DNS is public, individual transactions made by an end user **should not** be public.
- However DNS queries are sent in **clear text** (using UDP or TCP) which means passive eavesdroppers can observe all the DNS lookups performed.
- The DNS is a globally distributed system that crosses international boundaries and often uses servers in many different countries in order to provide resilience.
- It is well known that the NSA used the MORECOWBELL and QUANTUMDNS tools to perform covert monitoring, mass surveillance and hijacking of DNS traffic.
- Some ISPs log DNS queries at the resolver and share this information with third-parties in ways not known or obvious to end users.
- Some ISPs embed user information (e.g. a user id or MAC address) within DNS queries that go to the ISPs resolver in order to provide services such as Parental Filtering. This allows for fingerprinting of individual users.
- Some CDNs embed user information (client subnets) in queries from resolvers to authoritative servers (to geo-locate end users). This allows for correlations of queries to particular subnets.
- Note that even when using a VPN some VPNs will still leak your DNS queries by sending them unencrypted to your ISP. Use the nice tool from anonymyster.com to check is this is happening with your VPN!

An overview of the problems is given in this Tutorial: DNS Privacy Tutorial.

For an expert review of this topic recommended reading is DNS Privacy Considerations.

The solution?

For a full discussion of the options available please see DNS Privacy - The Solutions.

Client (stub) to recursive resolver

The two most widely deployed solutions for stub to recursive resolution are DNS-over-TLS and DNS-over-HTTP; they both encrypt DNS data and prevent passive surveillance of network data revealing users' DNS queries. They can both allow users to validate the server they choose for their DNS service to make sure they are using a provider who has a good privacy policy for how they handle user data. But they do have some different protocol properties and in practice are being deployed in somewhat different ways at the moment. Neither of these are trivial changes in the way DNS works and encryption of all DNS queries by default will not happen overnight.

See DNS Privacy Clients, DNS Privacy Implementation Status, DNS Privacy Public Resolvers, DNS Privacy Test Servers for more information.

Recursive resolver to Authoritative server

The DPRIVE working group at the IETF has been working on solutions for that, if you are interested see the DPRIVE mailing list.

SNI

Unfortunately the Server Name Indicator header in HTTPS messages also reveals the name of the website contacted by the user so provides a similar leakage channel for web traffic as the DNS queries. However there is work underway in the TLS working group at IETF to encrypt the SNI: I-D: Encrypted Server Name Indication for TLS 1.3.