Welcome to the DNS Privacy project home page

This site is the home of a collaborative open project to promote, implement and deploy DNS Privacy. The goals of this project include:

- Raising awareness of the issue of DNS Privacy
- Empowering users to take advantage of DNS Privacy tools and resources (client applications, DNS Privacy resolvers)
- Evolving the DNS to support DNS Privacy in particular developing new DNS Protocol standards
- Working towards full support for DNS Privacy in a range of Open Source DNS implementations including: gotdns, Unbound, NSD, BIND and Knot (Auth and Resolver)
- Co-ordinating deployment of DNS Privacy services and documenting operational practices

Among the many contributors to this project are Sinodun IT, NLnet Labs, Salesforce, Surfnet, NLnet Foundation, OTF, Stephane Bortzmeyer and No Mountain Software.
See past DNS Privacy work

December 2019:
- Good update on the latest DoH status for major browsers
- Official NGINX guide to how to set up DoT and DoH

November 2019:
- Microsoft announce plans to implement DoH in Windows... at some point: Windows will improve user privacy with DNS over HTTPS
- Paul Vixie's talk on DoH at NANOG77: DNS WARS: Episode IV A New Bypass
- Letter to US Congress regarding Chrome DoH plans
  - EFF and partners write in support of DoH
  - Mozilla ask congress to investigate ISPs use of consumer data
- Latest version of DNS Privacy Requirements for Exchanges between Recursive Resolvers and Authoritative Servers from the IETF DPRIVE WG
- Latest proposals on 'Adaptive DNS' from DPRIVE WG

October 2019
- Comcast begin a phase one of a DoH public beta: https://doh.xfinity.com/dns-query and a DoT public beta: dot.xfinity.com
- ICANN OCTO document including evaluation of encrypted DNS: Local and Internet Policy Implications of Encrypted DNS
- Mozilla release FAQ on DoH: DNS over HTTPS FAQs.
- DNSCrypt implements a scheme similar in concept to Oblivious DNS ANONYMIZED DNSCRYPT
- Nice article on DNS Security: Threat Modeling DNSSEC, DoT, and DoH from netmeister.org
- Netherlands National Cyber Security Centre publishes a factsheet on DNS monitoring Factsheet DNS monitoring will get-harder
- Opera announces experimental support fro DoH on an opt-in basis.

September 2019
- Another blog from Bert Hubert: Centralised DoH is bad for privacy in 2019 and beyond
- IMC Paper: An Empirical Study of the Cost of DNS-over-HTTPS
- And today the Encrypted DNS Deployment Initiative launches: "a collaborative effort to ensure the smooth global adoption and reliable operation of DNS encryption technology."
- Chrome announces experiment to upgrade to DoH with existing DNS provider
- OpenBSD has disabled DoH in their Firefox packages
- Firefox announce rollout of DoH by default in the USA during September.... and it will use Cloudflare
  - And a non-standard method to disable it....
  - And details of how to do this in BIND
- And..... some reaction about the Firefox DoH announcement...
- CircleID - http://www.circleid.com/posts/20190906_dns_over_https_the_privacy_and_security_concerns/

Overview of DNS Privacy Status

High level overview of ongoing work on DNS Privacy with monthly updates

DPRIVE Working Group

Catch up with the latest standards being developed to support DNS Privacy: DPRIVE Working group

Contact

If you are interested in contributing to the project please contact:
- Sara Dickinson (sara@sinodun.com)
- Allison Mankin (allison.mankin@gmail.com)
- Benno Overeinder (benno@NLnetLabs.nl)

We now have a twitter account: and a YouTube channel
Reference Material

For a list of useful RFCs, Internet Drafts and presentations see the Reference Material page.

Support

Thanks to NLnet Foundation and OTF for donations to support DNS Privacy work. Thanks for past support from Verisign Labs.

Comments, JIRA and Bitbucket Access

After a spate of spam comments we have reluctantly change permissions so that commenting on pages requires a user account. An account also provides access to submit general privacy issues in the issue tracker and contribute to the code repositories create a user account (note that Stubby has it's own issue tracker in github):

Sign up for a user account