DNS Privacy - Ongoing Work

This page described at a high level the progress in various areas of DNS Privacy work (most recent activity at the top)

March 2017

- Great work at the IETF 98 Hackathon on DNS Privacy. In particular see Stephane Borztmeyer's blog on his DNS-over-TLS monitoring plug-in.
- Proceedings from the NDSS DNS Privacy workshop are available here.
- Thanks to Matthew Ford from ISOC for a great write up of the workshop.
- We'll be talking at OARC about dnsprivacy.net

February 2017

- We are very pleased to announce a new donation from NLnet Foundation to support work on Stubby. Thank you for your generous support!!
- Preliminary agenda published for NDSS DNS Privacy Workshop (26th Feb, San Diego)
- DNS Privacy will be a topic at the IETF 98 Hackathon - please come along!

January 2017

- Planning under way for the NDSS DNS Privacy workshop on 26th February in San Diego
- https://datatracker.ietf.org/doc/draft-ietf-dprive-dtls-and-tls-profiles/ has cleared WGLC
- 1.0.0 release of getdns (which supports DNS-over-TLS)
- Knot resolver 1.2.0 released with improved DNS-over-TLS support
- Warren Kumari has provided a Docker container for easy deployment of a DNS-over-TLS server!

December 2016

- Improved usability for Stubby planned for the 1.1.0-alpha3 release
- The content of this site is now available via the dnsprivacy.org site.
- CoreDNS now offers DNS-over-HTTPS (as well as DNS-over-TLS). Also see dingo if interested in DNS-over-HTTPS clients.

November 2016

- IETF 97 EDU team held a DNS Privacy Tutorial, which got coverage in both Heise and two articles in The Register: The_Register_2 2Nov, The_Register_6Dec
- More work at the Hackathon on Knot Resolver DNS Privacy implementation, TCP support in BIND and Stubby. A further DNS Privacy test server made available thanks to dkg.
- DPRIVE working group discussed a possible re-charter to focus work on the Resolver to Authoritative problem.
- DNS-over- HTTP(S) BOF held

October 2016

- 2 more test DNS Privacy resolvers made available (Thanks to Surfnet for resources!)
- getdns version 1.1.02-alpha released with a prototype implementation of Stubby - a DNS Privacy stub resolver
- https://datatracker.ietf.org/doc/draft-ietf-dprive-dtls-and-tls-profiles/ moved into Working Group Last Call
- https://datatracker.ietf.org/doc/draft-mayrhofer-dprive-padding-profile/ was published to propose specific policies for padding DNS packets
- https://datatracker.ietf.org/doc/draft-ietf-dnssd-privacy/ adopted by the DNS-SD working group

September 2016

- https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsodtls/ passed WGLC with status 'Experimental' and was submitted to IESG for review

August 2016

- WGLC starts for https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsodtls/

July 2016

- https://datatracker.ietf.org/doc/draft-bortzmeyer-dprive-step-2/ was published as a first step in describing the Resolver to Authoritative problem

June 2016

- OARC made a test DNS Privacy server available - many thanks!

May 2016

- Presentation in the RIPE DNS working group on experimental deployments of DNS Privacy servers.
- RFC7858 Published: Specification for DNS over Transport Layer Security (TLS)

April 2016

- Work at the IETF Hackathon in Buenos Aires to start implementing TLS in Knot resolver

March 2016

- getdns 1.0.0b1 release!
- RFC7816 Published: DNS Query Name Minimisation to Improve Privacy

February 2016

- EDNS0 Keepalive draft approved for publication as RFC7828

January 2016

- 5966bis draft approved for publication as RFC7766
- *Authentication and (D)TLS Profile for DNS-over-TLS and DNS-over-DTLS* draft adopted by DPRIVE
- Testing of FreeBSD implementation of TCP Fast Open. Reported bug in linux client implementation of TFO (now fixed) and made feature request to OpenSSL to support client side TFO.
- Started work on Unbound patch to support TFO on Linux, FreeBSD and OS X.

December 2015

- Produced first version of *Authentication and (D)TLS Profile for DNS-over-TLS and DNS-over-DTLS* draft for submission to DPRIVE working group
- Client side EDNS0 keepalive option implemented in getdns
- SPKI pinset TLS authentication available in getdns

November 2105

- Attended IETF 94.
    - Participated in Hackathon including getdns implementation of EDNS0 Padding option
    - Last call review of DNS-over-TLS
    - Agreed to start work on combined draft for (D)TLS Authentication mechanisms

October 2015

- Attended OARC Fall Workshop. Presentationed onUsing TLS for DNS privacy in practice.
- Attended ICANN in Dublin, presented on *DNSSEC for Legacy applications* including discussing DNS privacy features of getdns.

August 2015

- Addition of TLS authentication using hostname to getdns

July 2015

- IETF 93
    - Work on getnds TLS authentication during Hackathon
    - Working group presentations on 59966-bis draft and https://tools.ietf.org/html/draft-ietf-dnsop-edns-tcp-keepalive-02
- 0.3 release of getdns including
    - New transport list options allowing user to flexibly specify an ordered list of accepted transport options from TLS, STARTTLS, TCP, UDP
    - Ability to configure idle timeout associated with TCP connections

May 2015

- 0.2 release of getdns including STARTTLS

April 2015

- Release of version 0.1.8 of getdns including TLS and TLS with fallback to TCP

March 2015

- Work started in getdns to implement dns-over-tls - Demo given at IETF92 in Dallas of proof-of-concept code.
- Publication of updated set of patches in the dns-over-tls repository
- Publication of https://tools.ietf.org/html/draft-ietf-dnsop-5966bis-01

January 2015

- Changed to using DNS-over-TLS instead of T-DNS
- Extend LDNS and NSD patches to include options to use the TO bit (for experimental inter-op testing)
- Publish LDNS code into repository for review
- getdns work put on hold, instead start work on Unbound server patch

November 2014

- Presenting at IETF 91
- Started work on T-DNS in getdns

October 2014

- Implementation of TCP Fast open support (linux only) in getdn for stub mode in 0.1.5 release.
- Testing of 0.1.5 getdns codebase which implements TCP pipelining.
- POC implementation of TCP Fast Open in ldns, Unbound and NSD.
- Patch released to implement STARTTLS in NSD.
- Released patch to ldns for connection re-use.

September 2014

- Continued helping to implement switch to ldns for stub mode in getdns.
    - Basic support for synchronous API implemented and per query namespaces also supported. (Note DNSSEC stub validation is still done by unbound at this point....)

- Creating patch for ldns/drill to support connection reuse for TCP. Using this from synchronous stub mode in getdns to demonstrate connection re-use.
- Work on TCP related drafts

August 2014

- Working on getnds
    - Added a new test to verify which transport queries are actually sent over
    - Helping to implement the switch to ldns for stub mode
    - Working on support for pipelining of TCP queries

July 2014

- Attended IETF 90 in Toronto and gave a demo of sending queries from drill to Unbound using T-DNS
- Started looking at pipelining multiple queries from drill to Unbound
- Extending test framework to test multiple scenarios for drill <-> Unbound
- Finished patch to drill to add extra options:
    - -l will send a single query over TLS
    - -L will send a single query over TLS after negotiating an upgrade using a STARTTLS/CH/TXT query
- Finished patch to Unbound to support 'upgrade_tls' configure option. This enables unbound to receive a a STARTTLS/CH/TXT query, send a STARTTLS/CH/TXT response when configured properly, upgrade to SSL and then receive a query over SSL.

June 2014

- Started work on Unbound <-> NSD hop
- Completing implementation in Unbound to get drill <-> Unbound hop working
- Implemented a patch to drill to support T-DNS for a single DNS query
- Discussions on the class to be used for the dummy query. The resolver -> authoritative hop might be better implemented with a IN class query.
- Start work on Unbound - understand current SSL-upstream implementation
- From Willem: LDNS does not have support for asynchronous operation so in the short term it will probably be used in getdns just in synchronous mode so that the implementation of TDNS can continue.
- Further work on test framework

May 2014

- Current getdns stub implementation cannot support sending of CH class queries as it uses libunbound which denies the query and never sends it onwards. Discussed in getnds meeting 19th May that further implementation of T-DNS in getdns will have to wait until libunbound is replaced with ldns for the stub mode. Current understanding is that Willem is going to tackle this in the next few weeks.
- Identified need to support CH class in getdns for dummy STARTTLS query. Start on implementation of this.
    - This implementation highlighted the need for getdns to gracefully handle refused queries that have no associated data.
- Created test harness to create a dummy STARTTLS query
- Agreed that initial implementations will use the dummy CH class query (not the TO bit)
- Forked getdns. Familiarisation with getdns code base - get it to install and run!
- Kick off meetings with T-DNS and getdns teams
- Creation of project issue tracker and wiki site
- Reading of relevant drafts and documentation - capture any early technical questions