Stubby

Willem Toorop
NLnet Labs

Sara Dickinson
Sinodun

Allison Mankin
Salesforce

NANOG68 Dallas, Texas

Genesis

- *getdns* is a modern async *DNS API* specification
- Designed by and for application developers
- First specification by Paul Hoffman 2013
- First library implementation by a collaborative effort: Verisign Labs, NLnet Labs, Sinodun, No Mountain Software and many others:

Claus Assman, Theogene Bucuti, Andrew Cathrow, Neil Cook, Saúl Ibarra Corretgé, Craig Despeaux, John Dickinson, Sara Dickinson, Robert Edmonds, Angelique Finan, Simson Garfinkel, Daniel Kahn Gillmor, Neel Goyal, Bryan Graham, Robert Groenenberg, Paul Hoffman, Scott Hollenbeck, Shumon Huque, Jelte Janssen, Guillem Jover, Shane Kerr, Anthony Kirby, Olaf Kolkman, Sanjay Mahurpawar, Allison Mankin, Sai Mogali, Linus Nordberg, Benno Overeinder, Joel Purra, Tom Pusateri, Prithvi Ranganath, Rushi Shah, Vinay Soni, Melinda Shore, Bob Steagall, Andrew Sullivan, Ondřej Surý, Willem Toorop, Gowri Visweswaran, Wouter Wijngaards, Glen Wiley, Paul Wouters

Some features of getdns

- Act as *stub* and *full recursive* ...libunbound
- *DNSSEC as stub*

  even without validating upstreams
- *Avoids DNSSEC roadblocks*

  works around upstreams that hamper DNSSEC
- *DNS64*

  signed IPv4 only names can be validated too
- *DNS Privacy*

  DNS over TLS

```
RFC7766  dns-over-tcp
RFC7858  dns-over-tls
RFC7830  eds0-padding
draft-ietf-dprive-dtls-and-tls-profiles
```

Some features of getdns

- Act as *stub* and *full recursive* ...libunbound
- *DNSSEC as stub*

  even without validating upstreams
- *Avoids DNSSEC roadblocks*

  works around u
- *DNS64*

  signed IPv4 o
- *DNS Privacy*

  DNS over TLS

These are all interesting for any application!

RFC7830 edns0-padding

draft-ietf-dprive-dtls-and-tls-profiles

Some features of getdns

- Ac
- A
- A
- A
- A

getdns_query

```
$ getdns_query -h
usage: getdns_query [<option> ...] \
    [@<upstream> ...] [+<extension> ...] \
    ['{ <settings> }'] [<name>] [<type>]

default mode: recursive, synchronous resolution of NS record
       using UDP with TCP fallback

upstreams: @<ip>[%<scope_id>][@<port>][#<tls port>][~<tls name>][^<tsig spec>]
            <ip>@<port> may be given as <IPv4>:<port>
                  or '['<IPv6>[%<scope_id>]']':<port> too

tsig spec: [<algorithm>:]<name>:<secret in Base64>
```

- Command line test tool used with getdns development

draft-ietf-dprive-dtls-and-tls-profiles

Some features of getdns

- Act as *stub* and *full recursive* ...libunbound
- *DNSSEC as stub*

  even without validating upstreams
- *Avoids DNSSEC roadblocks*

  works around upstreams that hamper DNSSEC
- *DNS64*

  signed IPv4 only names can be validated too
- *DNS Privacy*

  DNS over TLS
- **Since getdns 1.1.0-a1: *request handling***

Meet Stubby

We have all these stub features

A `getdns_query` tool that can use them all

Since getdns 1.1.0-a1 request handling funcs +

`getdns_query` can act as a *local stub server*

Stubby == `getdns_query`

Same program , different name
, different defaults

Building Stubby

- Requirement: OpenSSL 1.0.2 or later

```
~$ wget https://getdnsapi.net/dist/getdns-1.1.0-a2.tar.gz
getdns-1.1.0-a2.tar. 100%[===============>] 842,41K 402KB/s in 2,1s

~$ tar xf getdns-1.1.0-a2.tar.gz
~$ cd getdns-1.1.0-a2/
~/getdns-1.1.0-a2$ ./configure --without-libidn --enable-stub-only
…
~/getdns-1.1.0-a2$ make
…
~/getdns-1.1.0-a2$ sudo make install
[sudo] password for djb: ******
…
~/getdns-1.1.0-a2$
```

- Here configured for minimal dependencies for Privacy DNS

Configure Stubby

- Stubby reads config from

  `/etc/stubby.conf`
  `$HOME/.stubby.conf`

DNS over TLS: Opportunistic

```
{ dns_transport_list: [ GETDNS_TRANSPORT_TLS ]
, upstream_recursive_servers:
  [ 184.105.193.78, 2620:ff:c000:0:1::64:25 ]
}
```

DNS over TLS: Strict

```
{ dns_transport_list: [ GETDNS_TRANSPORT_TLS ]
, tls_authentication: GETDNS_AUTHENTICATION_REQUIRED
, upstream_recursive_servers:
  [ 185.49.141.38~getdnsapi.net ]
}
```

Configure Stubby

- Stubby reads config from

  `/etc/stubby.conf`
  `$HOME/.stubby.conf`

DNS over TLS: Strict with SPKI pinset auth.

```
{ dns_transport_list: [ GETDNS_TRANSPORT_TLS ]
, tls_authentication: GETDNS_AUTHENTICATION_REQUIRED
, upstream_recursive_servers:
  [ { address_data: 185.49.141.38
    , tls_pubkey_pinset:
      [ { digest: “sha256”
        , value: 0x7e8c59467221f606695a797ecc488a6b4109
dab7421aba0c5a6d3681ac5273d4 } ]
  } ]
}
```

Running Stubby

- `-g` option runs Stubby in background
  pid file in `/var/run/stubby.pid`

```
~$ sudo stubby -g
~$
```

Test Stubby:

```
~$ dig @127.0.0.1 nanog.org
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10093
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 7, ADDITIONA

;; QUESTION SECTION:
;nanog.org.            IN A

;; ANSWER SECTION:
nanog.org.      579   IN A  50.31.151.73
```

Modify upstream resolvers

- Edit `/etc/resolv.conf`

/etc/resolv.conf

```
nameservers 127.0.0.1
nameservers ::1
```

on OS X:

```
~$ sudo networksetup -setdnsservers Wi-Fi Empty
~$ sudo networksetup -setdnsservers Wi-Fi 127.0.0.1 ::1
```

Go Stubby!

- Stable release before 2017

Sergeant Stubby *(July 21, 1916 – March 16, 1926), was the official mascot of the 102nd Infantry Regiment (United States), assigned to the 26th (Yankee) Division. Stubby served for 18 months and participated in seventeen battles on the Western Front. He saved his regiment from surprise mustard gas attacks, found and comforted the wounded, and once caught a German soldier by the seat of his pants, holding him there until American soldiers found him.*

(source: https://en.wikipedia.org/wiki/Sergeant_Stubby)