DNS Team

IETF 97 Hackathon

Participants (new to IETF / ***new to Hackathons***)

John Dickinson

Sara Dickinson

Daniel Kahn Gillmor

Dave Lawrence

Allison Mankin

Carlos Martinez

Michel Odou

Benno Overeinder

Matt Pounsett

Daniel Shaw

Melinda Shore

Ondře Surý

Overview of activities

Motivation:

- Improved privacy in using DNS services on the Internet
- Implementation of DPRIVE drafts/RFCs

How:

- Securing/encrypting stub to resolver DNS transactions
- DNSSEC/DANE for authenticated TLS
  - for DNS and (any) other communication
- Anti-traffic analysis padding
- ...

Highlights

Stubby (privacy and security on client host)	Testing, Interop testing, Outreach Planning (Michel, Benno, Allison, Sara)
Stub <-> Recursive	Anti-Traffic Analysis Padding: Knot Recursive Server (dkg, Ondřej)
Stub <-> Recursive OOOP (for TCP/TLS)	Unbound Implementation in Progress (Willem)
Stub <-> Recursive OOOP Test Support	Server: ###.delay.getdnsapi.net (Willem)
Python Bindings New Function	File-to-List (Matt)
Recursive	Ephemeral Certs in Knot (dkg, Ondřej)

Stubby stub resolver

Stand-alone getdns stub resolver

- IPv6 prefix synthesis (DNS64)
- Roadblock avoidance
- DNS privacy
  - TLS authentication (strict/opportunistic)
- ...

Interoperability tests with public/open privacy-enhanced resolvers

- Unbound
- Knot resolver
- Bind with ngix

Ephemeral Certs and Padding

Knot resolver:

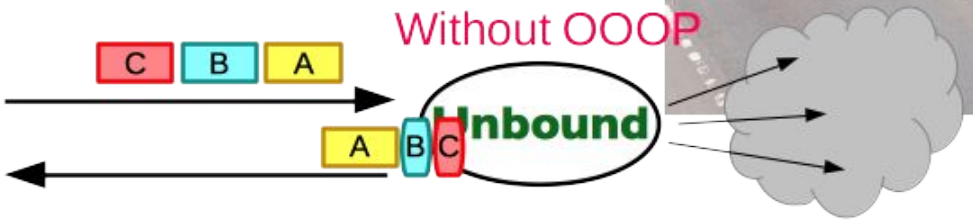
- Ephemeral Certs for DNS over TLS implemented
- ENDS0 padding for DNS over TLS *just* finished
    - anti-traffic analysis padding

Out Of Order Processing (OOOP)

for Unbound

With TLS stateful no longer fallback transport
- keep connections open
- pipelining of queries

Without OOOP



With OOOP!

`delaydns` - Reliably test Out Of Order Processing (OOOP)

Query for:

`<delay in miliseconds>.delay.getdnsapi.net`