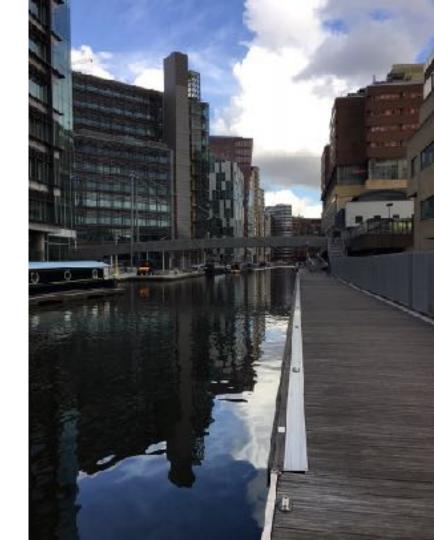
IETF Hackathon: DNS, DNS-SD, DPRIVE, & DOH

IETF 101 17-18 March, 2018 London



Hackathon Plan

• DoH: DNS-over-HTTPS. Multiple implementations + inter-op of draft-ietf-doh-dns-over-https-03

people

~50/50 split of

 DNS, DNS-SD & DPRIVE: Many small projects

What got done: DoH

Work in Progress: More details in the <u>DOH branch of theIETF GitHub repo</u>

Language	Code	Client	Server	Who
C	<u>getdns</u>	Υ		Willem Toorop
Go	Go DNS CoreDNS	-	-	Miek Gieben
Python/C	github	Υ	Y	Stéphane Bortzmeyer
Python	<u>github</u>	Υ	Υ	Manu Bretelle
nginx + Lua	<u>github</u>		Υ	Tony Finch
C + PHP	<u>github</u>	Υ	Υ	Massimiliano Fantuzzi
Javascript	<u>github</u>	Υ		Tom Puseteri
Python	<u>Test System</u>	-	-	Manu Bretelle

What we learned: DoH

- Full report planned at the DOH working group
- HEADLINE: Mostly it works!
 - Inter-op was OK (also with public DoH servers).
- Draft updates:
 - GET/POST SHOULD vs MUST might need to be specified...
 - Error handling is unspecified needs to be
- Minor clarifications/bugs
- DoH not a good fit for Go DNS library (TLS was)
- Plus you can write a Perl DoH client in 20 lines of code!

DNS and HTTP folks talked!!

What got done: DNS/DNS-SD

- DNS-Service Discovery (Ted Lemon + Stuart Cheshire)
 - draft-sctl-dnssd-mdns-relay

DNS/DNSSEC

- DNSSEC/IXFR: implementation draft-mekking-mixfr (expired).
 Reduces bandwidth. Goal was measurements resurrect draft?
- Perl Net::DNS::SEC: Edwards curve validation (RFC8080)
 - Epic fail! Acknowledgements to Nick Harper (ASN1 surgeon)
- KSK Sentinel: draft-ietf-dnsop-kskroll-sentinel issues found
- ANAME: draft-ietf-dnsop-aname

What got done: DPRIVE

• **getdns/Stubby**: connect to resolver by name (*draft-ietf-dprive-dtls-and-tls-profiles*)

```
upstream_recursive_servers:
# The SB's HTTPS server:
  - uri: "https://dns.bortzmeyer.fr"
# The quad9 DNS over TLS server
  - name: "dns.quad9.net"
```

- (RFC7858) DNS-over-TLS
 - systemd-resolved: forwarding stub configuration work started
 - BIND: DNS-over-TLS, libidn 2008 support
 - dnsperf: Adding TLS support for benchmarking
 - EDNSO Padding: (RFC7830) in Tenta, pydig, CoreDNS
- TLS DNSSEC Chain Ext: (draft-ietf-tls-dnssec-chain-extension) demo server code, all nameservers of andreasschulze.de, signing-milter.org or openarc.org

Teams

DNS Team members:

- Shane Kerr
- Matthijs Mekking
- Dick Franks
- Evan Hunt
- Petr Špaček

DPRIVE Team members:

- Willem Toorop
- Jim Hague
- Sara Dickinson
- Ondřej Surý
- Daniel Kahn Gillmor

Remote DPRIVE:

- Andreas Schulze
- Logan Velvindron

First timers @ Hackathon:

- Tony Finch
- Massimiliano Fantuzzi
- Logan Velvindron
- Dick Franks
- Matthijs Mekking