DNS Team

IETF 100 Hackathon

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

Manu Bretelle

Francis Dupont

Martin Hoffmann

Dave Lawrence

Allison Mankin

Benno Overeinder

Hans Seidel

Mukund Sivaraman

Ondře Surý

Willem Toorop

Highlights

DNS-over-TLS in Bind	First prototype, not finished yet (Mukund and Ondrej)
DNS-over-HTTPS	Prototype/proof-of-concept implementation (Manu)
DANE authentication of TLS upstreams	Protoype in getdns Stubby, will be finished by Wednesday for demo in Code Lounge (Willem)

DNS-over-TLS in Bind

- Made a good start in implementing DNS-over-TLS
  - Complex feature to implement, but clear approach and path-forward now
  - Implementation will be completed after IETF meeting
  - With Bind, now three open-source implementations implement DNS-over-TLS (with Unbound and Knot Resolver)

- RFC 7858, Specification for DNS over Transport Layer Security (TLS)

DNS-over-HTTPS Proxy

- Python scripts that supports proxying DNS over HTTPS to a recursive resolver.
- https://github.com/chantra/doh-proxy

Caveats

- currently standard HTTP1 is used, next step will be to look into aioh2/hyper-h2
- 1 request per connection only

DoH WG

- Draft-ietf-doh-dns-over-https

Test client (sigfail)

```
$ cd dohproxy
  $ python3 ./client.py  --domain dns.dnsoverhttps.net --qname sigfail.verteiltesysteme.net  --dnssec
  id 37762
  opcode QUERY
  rcode SERVFAIL
  flags QR RD RA
  edns 0
  eflags DO
  payload 4096
  ;QUESTION
  sigfail.verteiltesysteme.net. IN AAAA
  ;ANSWER
  ;AUTHORITY
  ;ADDITIONAL
```

Test Client (sigok)

```
$ python3 ./client.py  --domain dns.dnsoverhttps.net --qname sigok.verteiltesysteme.net  --dnssec
  id 49772
  opcode QUERY
  rcode NOERROR
  flags QR RD RA AD
  edns 0
  eflags DO
  payload 4096
  ;QUESTION
  sigok.verteiltesysteme.net. IN AAAA
  ;ANSWER
  sigok.verteiltesysteme.net. 60 IN AAAA 2001:638:501:8efc::139
  sigok.verteiltesysteme.net. 60 IN RRSIG AAAA 5 3 60 20180130030002 20171031030002 30665 verteiltesysteme.net.
  O7QgNZFBu3fULvBXwM39apv5nMehh51f mLOVEsC8qZUyxIbxo4eDLQt0JvPoPpFH 5TbWdlm/jxq5x2/Kjw7yUdpohhiNmdoD
  Op7Y+RyHbf676FoC5Zko9uOAB7Pp8ERz qiT0QPt1ec12bM0XKQigfp+2Hy9wUuSN QmAzXS2s75k=
  ;AUTHORITY
  ;ADDITIONAL
```

DANE Authentication of TLS Upstreams

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