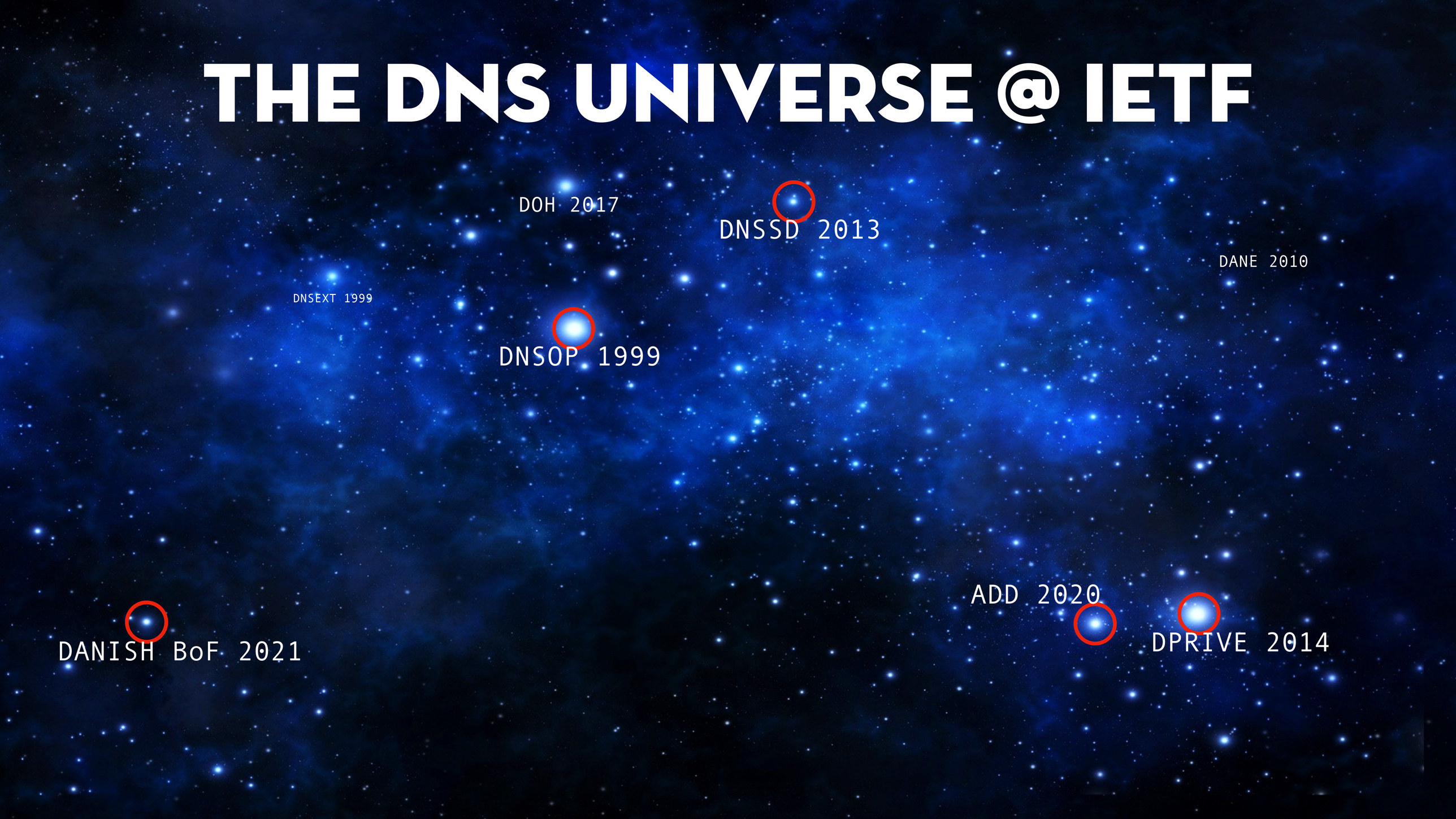
KEEPING UP WITH THE IETF DNSOP WG

Benno Overeinder

OARC 35, May 7, 2021


THE DNS UNIVERSE @ IETF
DOH 2017
DNSSD 2013
DANE 2010
DNSEXT 1999
DNSOP 1999
ADD 2020
DPRIVE 2014
DANISH BoF 2021

FINISHED WORK IN DNSOP @ IETF110

- Message digest for DNS zones (RFC 8976)
  - integrity of zone file and origin authenticity
  - use-cases: root zone, response policy zones, centralised zone data service (CDZS), …
- DNS Server Cookies (RFC 9018)
  - lightweight DNS transaction security mechanism, update RFC 7873 for interoperability (anycast)
  - protect against amplification attack, forgery, off-path cache poisoning

ALMOST FINISHED WORK IN DNSOP (1)

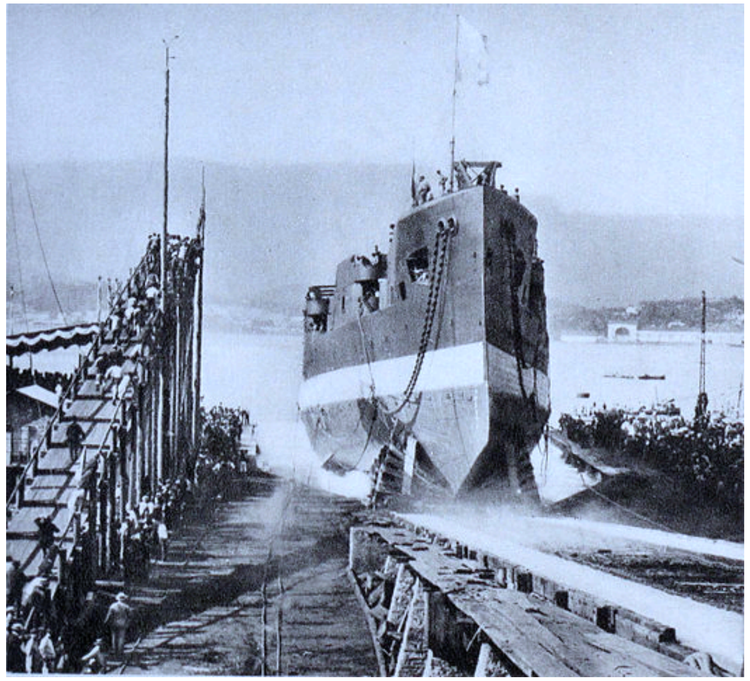
Working Group Last Call

- Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)
  - new type of records allowing a client to learn more about end-point service before connecting
  - improve security, privacy and performance (*and enable aliasing of apex domains*)
- DNS Transport over TCP - Operational Requirements
  - for DNS over unencrypted TCP, as well as over an encrypted TLS session

ALMOST FINISHED WORK IN DNSOP (2)

Close to WGLC

- Revised IANA Considerations for DNSSEC
  - updates RFC 5155 and RFC 6014, which have requirements for DNSSEC algorithms
  - motivation: relieving the need to make every national crypto algorithm an IETF standard just for DS records



Closed WGLC

- DNS Query Name Minimisation to Improve Privacy, draft-ietf-dnsop-rfc7816bis
- NSEC and NSEC3 TTLs and NSEC Aggressive Use

EXISTING DNSOP DRAFTS THAT NEED WORK

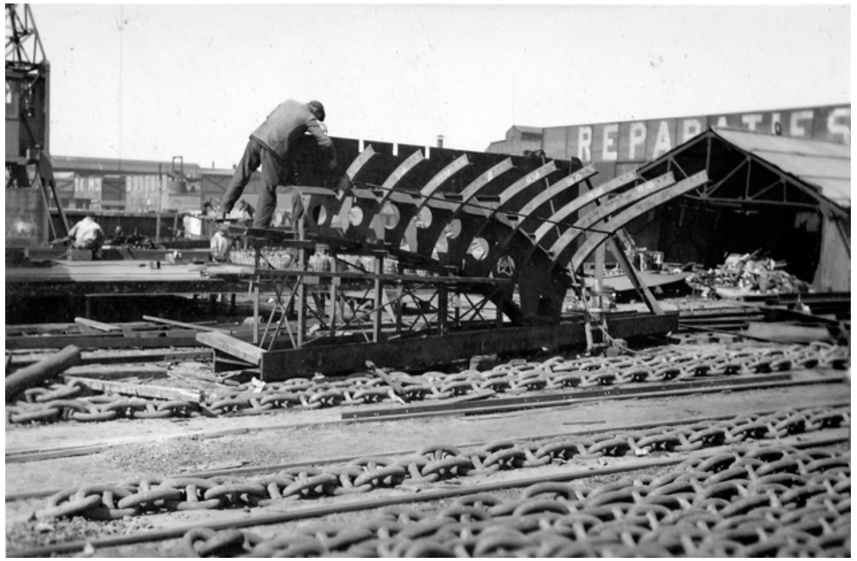
- DNS catalog zones
  - sync configuration from primary to secondary
  - generate zone file + XFR
  - questions to operators for use-cases
- DNS avoid fragmentation, max size interval?

Source	IPv4	IPv6
RFC 4035 (MUST/SHOULD)	1220/4000	1220/4000
DNS Flag Day 2020	1232	1232 (1280-40-8)
Measuring DFD 2020	1472 (1500-20-8)	1452 (1500-40-8)

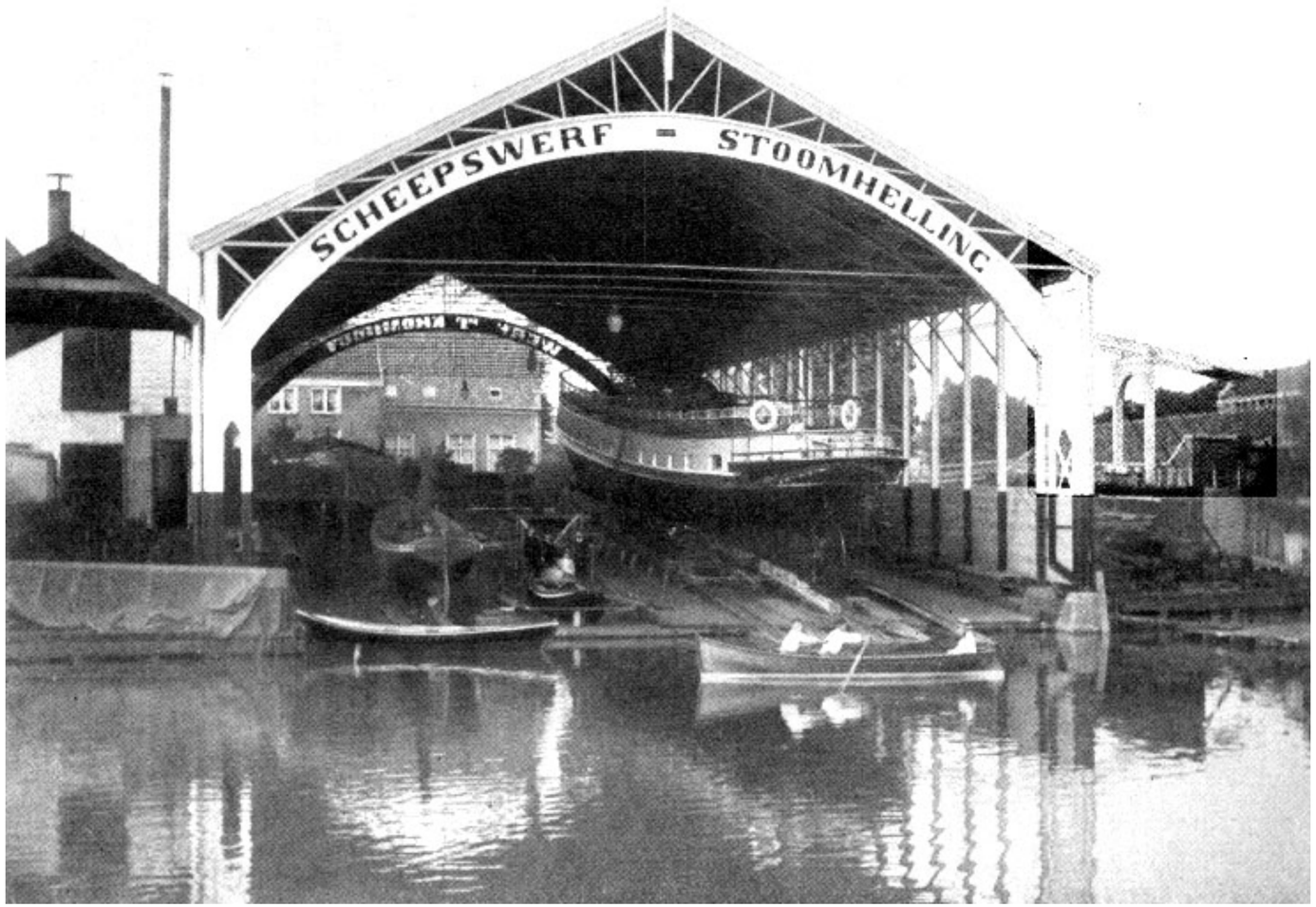
NEW WORK IN DNSOP

- NSEC3 Iteration Considerations
  - NSEC3 proof of non-existence, discorage zone enumeration
  - uses N iterations of a cryptographic hash, allows for the (optional) use of a salt
  - max limits set in RFC 5155
  - complex for authoritative engines, complex for validators: everyone suffers
- DNSSEC Automation
  - RFC 8901 Multi Signer DNSSEC Models
  - elegant insight using RFC 8901 for generic use-case changing NS operator for signed domains (without going insecure)

key size	old iterations	new iterations
1024	150	100
2048	500	100
4096	2500	100

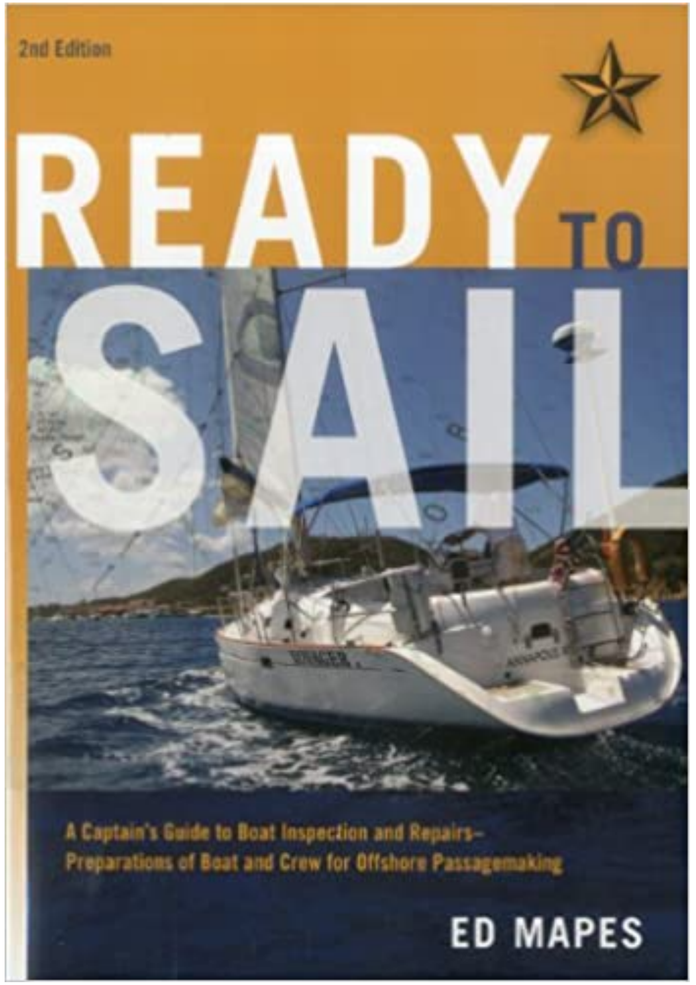


UPDATES FROM DPRIVE @ IETF110



ALMOST FINISHED WORK

- XFR-over-TLS (XoT) submitted to the IESG for publication



EXISTING WORK

- DNS-over-QUIC
  - ≠ DoH with HTTP/3, QUIC is a transport layer
  - DoQ stub-resolver, resolver-authoritative discovery similar to DoT
  - DoQ implementation status (table copied from presentation by Sara Dickinson)

implementation	language	notes
CoreDNS	Go	AdGuard uses as DoQ server
AdGuard DNS proxy	Go	Simply proxy server supporting DoQ
dnslookup	Go	Command line utility wrapper for Adguard DNS proxy
AdGuard C++ DNS libs	C++	AdGuard use in mobile app
Quicdoc	C	Simple DoQ impl based on Picoquic
aioquic	Python	QUIC impl. includes example DoQ client/server
Flamethrower	C++	DNS performance utility with experimental DoQ

EXISTING WORK (CONT'D)

February/March 2021

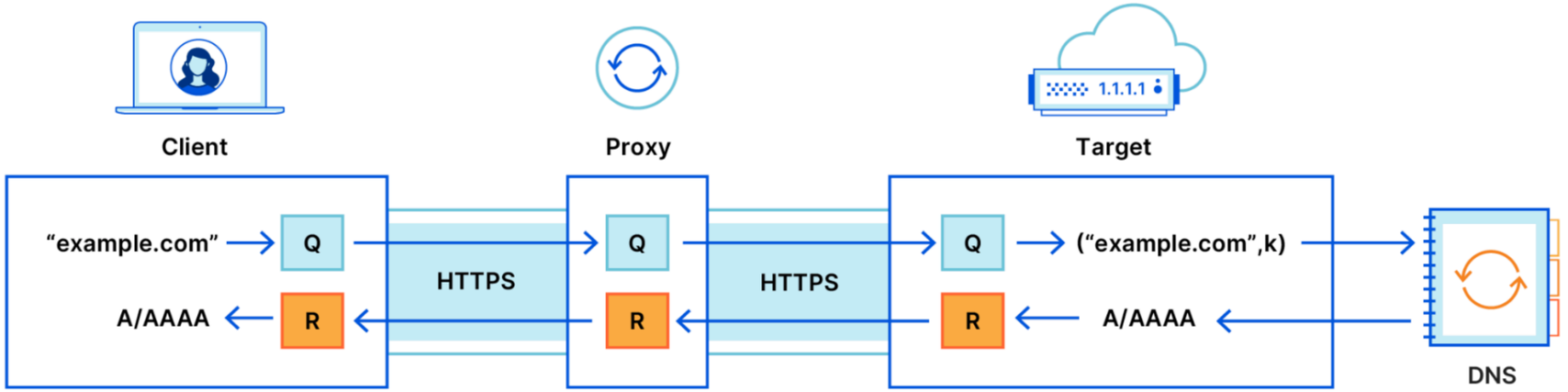
- Recursive to Authoritative DNS with Encryption

Today

- Recursive to Authoritative DNS with Unauthenticated Encryption
- *Common Features for Encrypted Recursive to Authoritative DNS*
- *Signalling Authoritative DNS Encryption*
  - *SVCB can be used to discover whether name server supports encryption*

DRAFT CONSIDERED FOR ISE

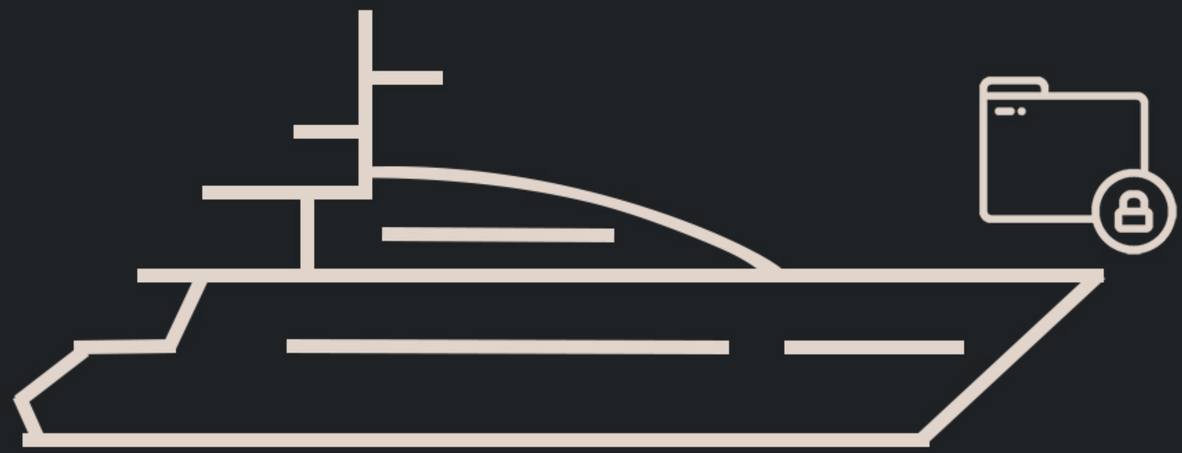
- Oblivious DoH (ODoH)



Picture from https://blog.cloudflare.com/oblivious-dns/

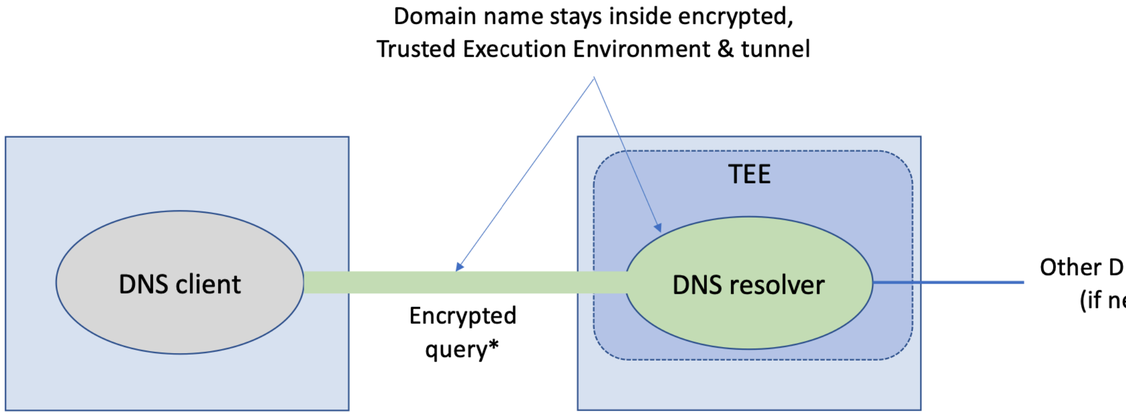
- Draft co-authored by Apple, Cloudflare and Fastly
- ODoH service launched in December 2020 by Cloudflare with partners: PCCW, SURF, Equinix (https://blog.cloudflare.com/oblivious-dns/)

CONFIDENTIAL DNS



USING CONFIDENTIAL COMPUTING TO PROTECT DNS RESOLUTION

- DNS privacy is a popular topic!
  - Domain name meta-data visible on the wire (even with encryption)
  - Resolvers have the potential too see user's entire browsing history
  - Large resolver services are an attractive target (public, operator, ...)
- Protect user's data in flight, at rest, or in use – we wanted to experiment with tech that could reduce leaks on the last two
- TEE: environment that enforces that any code within that environment cannot be tampered with, and that any data used by such code cannot be read or tampered with by any code outside that environment [ietf-teep-architecture]
- upsides/down sides discussion



* Can be built on top of DoT [RFC7858] or DoH [RFC8484]

THANK YOU
&
QUESTIONS?