DNS PRIVACY AND ENCRYPTION WHERE ARE WE?

John Levine

STANDCORE LLC

ROW 9 | Cyberspace

ALREADY STANDARDIZED

- Unencrypted DNS on port 53 (RFCs 1034, 1035, and many others)
- DNSSEC to validate results (RFC4033, 4034, 4035)
- DoT: DNS over TLS on port 853 (RFC 7858)
- DNS over DTLS on port 853 (RFC 8094, experimental)
- DoH: DNS over HTTPS usually on port 443 (RFC 8484)

WHERE ARE THEY USED?

- Stub to cache by private agreement
- DoT from stub to cache: not very popular yet
- DoH from stub to cache: widely used browsers, some other places
- No agreement on provisioning
  - Widely differing implementations: opt-in vs opt-out vs upgrade
  - Widely differing opinions on what problem it solves

STILL TO COME

- DoT or DoH from cache to authoritative
  - Needs a standard so any cache can talk to any authoritative
  - Need signal that a zone has DoT or DoH
  - Need agreed way to check that client is talking to the desired server
- Parent server will presumably signal to client that child does DoT or DoH
  - Hard to do without DNS changes
  - Probably will require provisioning at parent (hello, EPP!)

ENCRYPTED SERVER NAME INDICATION (ESNI)

- When a HTTPS server has multiple names, SNI leaks the name the client expects
- ESNI draft encrypts the name, but still can leak via DNS queries for the name
- DoH or DoT probably the best mitigation

DNS PRIVACY AND ENCRYPTION WHERE ARE WE?

John Levine

STANDCORE LLC

ROW 9 | Cyberspace