DPRIVE Implementers Perspective on Recursive to Authoritative

Benno Overeinder

IETF 102, Montréal, CA

Confidentiality of DNS Transactions

- Privacy ≠ confidentiality
  - QNAME minimization RFC 7816
    - Hide information from name servers
  - DNS-over-TLS (DoT) RFC 7858
    - On-path eavesdroppers

- Clear analysis of trade-offs
  - QNAME vs DoT, or both, with respect to RFC 7626
  - QNAME minimization by small resolvers with on-path eavesdroppers?
  - Distribution of queries to small vs. large number of resolvers
    - One operator collecting all information vs. many operators collecting *some* information

Explore Design Space

- From stub to recursive
  - DNS-over-TLS
  - DNS-over-DTLS
  - Confidential DNS [draft-wijngaards-dnsop-confidentialdns]

- From recursive to authoritative
  - Existing: DoT/DoD
  - New: DoH
  - Upcoming: DoHoQ, DoQ (Q for QUIC)
  - …

Authentication of Name Servers

- Authentication alternatives
  - Web PKI
    - CA stores and unknown CAs?
  - draft-bortzmeyer-dprive-resolver-to-auth
    - ietf-tls-dnssec-chain-extension
    - Open TLS → DANE record → authenticate → resolve

Operator perspective

- DoT at authoritative is not complex, but
  - Difficult to scale like UPD (vertical)
  - Scale with load balancer, TCP hand-off, more hardware (horizontal)

- Increased operational costs of DoT at authoritative
  - Will/can root operators and TLDs deploy this?
  - Mainly SLDs?
    - Which SLDs? Privacy/human right organizations
- Alternative deployment strategies
  - Root: hyperlocal root zone at the recursive
  - TLDs: local auth zone at the recursive