DNS-over-TLS and Root-Server Statistics

John Heidemann, Wes Hardaker, Yuri Pradkin
USC/ISI, B-Root Project
for the 2024 DINR Workshop
2024-04-04

Encryption fixes privacy, right?

(or DNS-over-TLS, DNS-over-HTTPS, DNS-over-QUIC, etc.)

not always:

- packet length analysis
- both ends have clear data => Root Op transparency: RSSAC-002 statistics

talk contributions:

- clarify threat model
- re: stats and reporting

DNS Threat Analysis

goal	problem	solution
confidentiality	**eavesdropping**	**dns-over-TLS!**
integrity	changing results	DNSSEC signatures
authenticity	results from owner	DNSSEC chain of trust to root
availability	denial-of-service	many servers and anycast
(non-repudiation)		not currently a goal

Root Operator Stats: RSSAC-002

- Root Operators agree to provide statistics: RSSAC-002
- goals
  - transparency about operations
    - what do you do?
    - how hard is it?
  - informing choices in policy and operations
    - how many sites do you need? where?
    - will DNS-over-{TLS,HTTPS,QUIC,etc.} increase latency much?

DNS-over-TLS and Stats

- how stats interact with privacy?
  - **stats are aggregate only**: how many queries? errors? queriers? etc.
  - data is from recursive resolvers, so **input is already aggregated**
- does RSSAC-002 require stats of queries from DNS-over-TLS?
  - not technically: RFC-9539 (TLS rec->auth) is experimental
- but RSSAC-002 *should* include DNS-over-TLS
  - stats address real operational needs!
  - we should minimize any privacy risk

the Query Lifecycle: with Stats *and* DNS-over-TLS

- **clients** query recursive resolvers
- **recursives** query authoritatives
  - aggregate queries
  - cache prior results
  - employ QName Minimization vs. authoratitives
  - employ DNS-over-TLS vs. third parties
- **authoritatives** handle queries
  - reply to recursives (the main job!)
  - observe with dnstap
- authoritative **analysis for stats** (B-Root's implementation)
  - dnstapmq: convert dnstap to simple TSV-format ("message-question")
  - dnsanon_rssac: slice into counts for RSSAC-002
    - separate querieres from query names
    - summarize counts across observers

our additions for TLS + stats

Privacy Across the Query Lifecycle

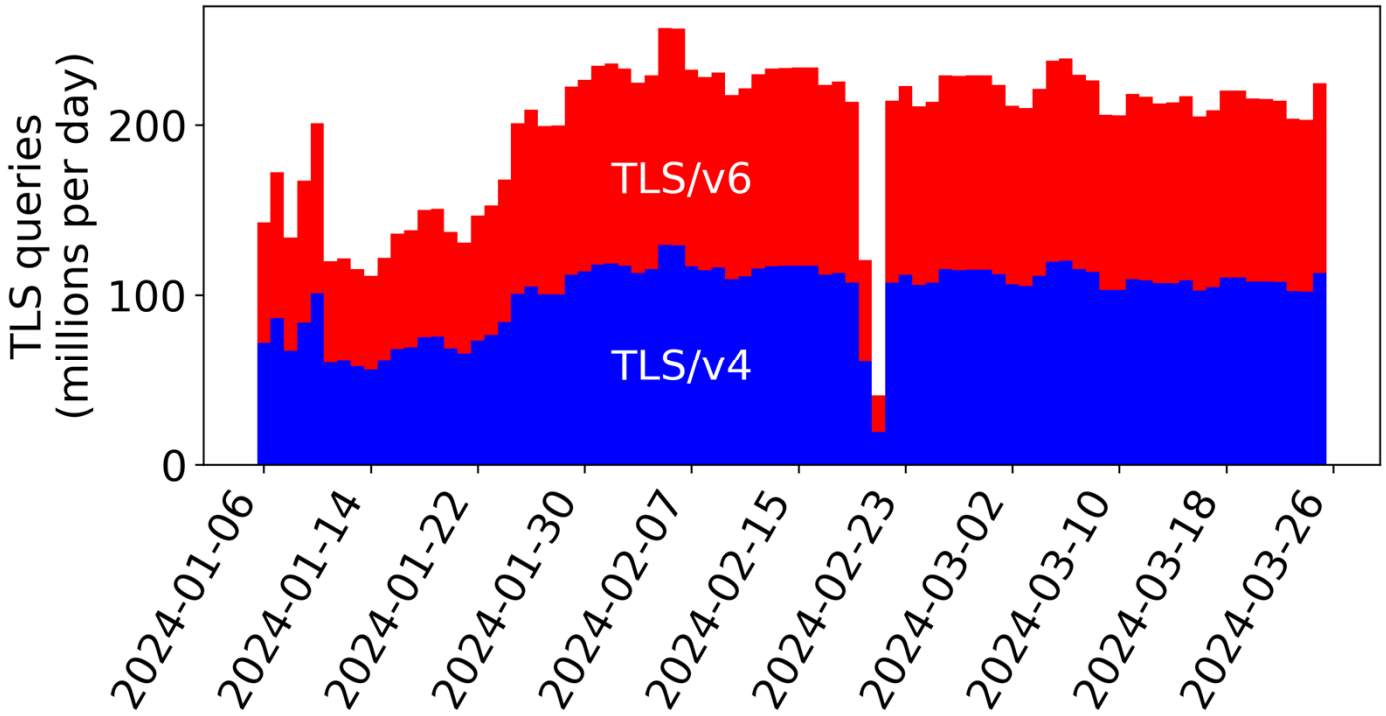
- **clients** query recursive resolvers
- **recursives** query authoritatives
  - aggregate queries from many users
  - cache prior results
  - employ QName Minimization vs. authoratitives
  - employ DNS-over-TLS vs. third parties
- **authoritatives** handle queries
  - reply to recursives (the main job!)
  - observe with dnstap
- authoritative **analysis for stats** (B-Root's implementation)
  - dnstapmq: convert dnstap to simple TSV-format ("message-question")
  - dnsanon_rssac: slice into counts for RSSAC-002
    - separate querieres from query names
    - summarize counts across observers

recursive resolvers have critical role in client privacy!

authoritatives observe for stats

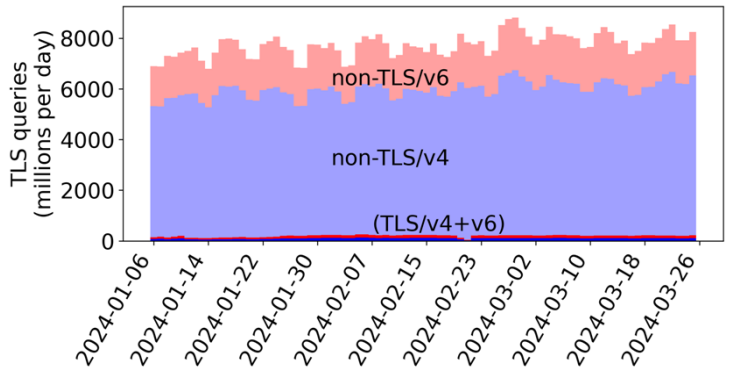
authoritatives separate querier (id) from query (name) quickly

Trends in DNS-over-TLS at B-Root



⇒ about 200M TLS queries/day
⇒ half v4, half v6
⇒ most from Google

⇒ about 2% of queries to B



Where from Here?

- DNS-over-TLS recursive->authoritative works!
- privacy in DNS is a team sport
  - DNS-over-TLS: confidentiality vs. third parties
  - recursive resolvers: critical player
    - aggregation, caching, Qname minimization
  - authoritatives should be careful in stat processing
- authoritatives should collect operational stats
  - our RSSAC-002 code is open-source
  - https://ant.isi.edu/software : dnsanon, dnsanon_rssac, dnstapmq