Query Name Minimization

Fred Baker (ISC)

Ken Renard (US Army Advanced Research Lab)

RFC 9156

DoT and DoH

- DoT and DoH are getting a lot of (well-deserved) attention for DNS privacy

Deployments in web browsers (DoH) are benefiting a large population of users

DoH looks like any other HTTP traffic and is harder to 'control' from the network path

DoT can easily be distinguished and possibly blocked since it uses dedicated port

- DoT and DoH are initially targeted for stub to recursive

Big gains in privacy for end users

Must trust recursive (stub offloads DNSSec validation to recursive)

memory/cpu overhead on stub and recursive

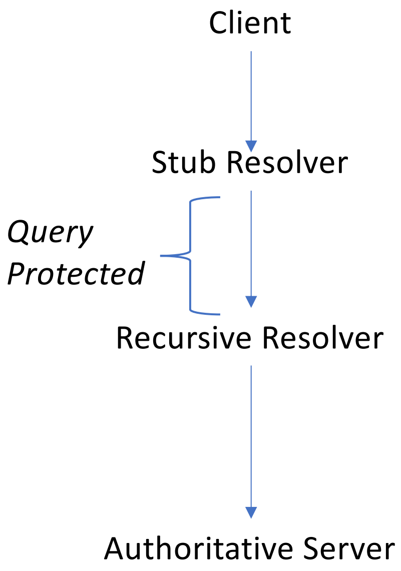
TCP overhead in network bandwidth and extra round trip(s)

as with any crypto, key management is important

stub (or application) configured with addresses of DoT/DoH capable recursives

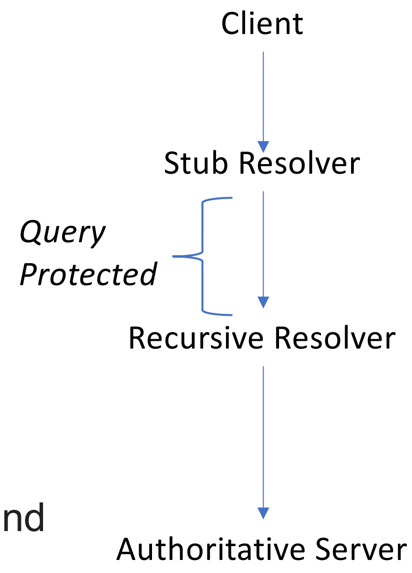
Using TLS encryption to enhance DNS query privacy #1

- **DNS over TLS (DoT) RFC 7858**
  - TCP, primarily for Stub resolver to Recursive resolver traffic
  - TLS, and therefore encryption
- Issues:
  - Each potential client knows suitable servers by address (configuration)
  - Each server maintains session state for each client using it (memory)
  - Attack: know the key in use
  - Bandwidth: TCP sessions use more bandwidth and memory than UDP sessions
  - Session computation: encrypt/decrypt implies overhead



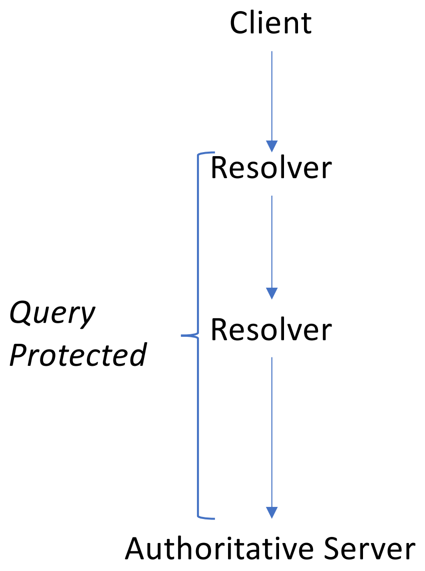
Using encryption to enhance DNS query privacy #2

- Alternative: DNS over HTTPS (DoH) RFC 8484
  - TCP, primarily for Stub resolver to Recursive resolver traffic
  - HTTPS, and therefore encryption
- Issues:
  - Each potential client knows suitable servers by address (configuration)
  - Each server maintains session state for each client using it (memory)
  - Attack: know the key in use
  - Bandwidth: HTTPS sessions use more overhead, bandwidth, and memory than UDP sessions
  - Session computation: encrypt/decrypt implies overhead



What if we don’t send the data?

- Alternative: Query Name Minimization RFC 9156
  - Any transport protocol – traditional DNS, DoT, or DoH
  - DNS client or resolver to the authoritative name server
  - Requires Query Name parsing by servers and resolvers on path
- Issues:
  - Uses a specialized port number (configuration)
  - Cache organization (sort by name passed along)
  - Attack: intercept point, if any, must be before label is removed



DNS Privacy between recursive and authoritative servers

Signaling mechanisms exist for recursive to discover DoT/DoH support from authoritative
Discovery adds overhead once per (X)
Significant infrastructure upgrades (authoritative servers) required good privacy

QName minimization available for recursives to limit exposure of DNS query strings

Recursive sends only the number of labels necessary to recurse through the hierarchy

example (".com" to root, "example.com" to .com, "www.example.com" to example.com)

Observers on path between recursive and authoritative can view query

Source of query is obfuscated among all users of recursive

Authoritatives only see the part of the query that they need to process the request

Deployment of QName Minimization

Done only by recursive resolver
Can be combined with DoT/DoH from stub-to-recursive
Can be combined with DoT/DoH from recursive-to-authoritative
No end-user requirement

QName minimization provides privacy measures at a fairly small cost

-

Recommendations

Configure recursive resolvers with QName minimization if possible
End-users can select trusted recursive resolvers that implement Qname minimization
Authoritatives can monitor the effects of Qname minimization