User Considerations for Recursive-to-Authoritative DNS-over-TLS

Paul Hoffman

IETF 102, Montréal

This is about use cases, not protocols

- Look first at what users need, not what is easy to do for developers
- One caveat: configuration for recursive and authoritative servers should be easy and not cause disruption to current services
- TLS seems likely, but is not a foregone conclusion

Two specific use cases

- Proposed use cases:
  1. Give some privacy between the resolver and authoritative servers for most current DNS users
  2. Give strong privacy and authentication between the resolver and authoritative servers for those users that require it
- These can use the same protocol, but the authentication is completely different
- There may additional use cases between these two

Give some privacy for most current DNS users

- Client sets up private session but does no authentication of the server
- Treats responses exactly the same as if they had come over port 53
- Advantage to users: prevents passive snooping of their queries from their resolvers
- Disadvantage to users: responses are probably a bit (or a lot) slower than port 53

Give users strong privacy and authentication

- Must authenticate the secure session
- The starting document might list examples of why a resolver might need strong privacy and/or authentication
- Individual use case documents would define how to implement for each use case
  - Searching among NS RRset
  - What to do if the resolver can’t authenticate at any NS
  - How to mark the fact that the response comes from an authenticated authoritative
  - . . .