DELEG for Encrypted DNS

Manu Bretelle

IETF 119, Brisbane AU, 19 Mar 2024
Current Limitations of NS

- **NS only carries minimal target information**
  - Only signals a target name, which itself only resolves to an IP
  - No indication of transport protocol, port, wire-format version...
  - Not extensible
  - One way direction, no negotiation

- **Multiple encrypted DNS transport protocols**
  - DoT, DoQ, DoH, DoH3
  - Support by both auth and recursive

- **Deployment is stalled**
  - Opportunistic probing (RFC9539). Doesn’t protect against active attackers.
  - Multiple attempts made with no success: Encoded in the name, signal in DS...

- **Need to signal features available downstream**
  - DS RR signals DNSSEC support
  - Adding more RR will cause continuous deployment pain
  - Need for a flexible and extensible way to augment metadata about downstream servers
  - Opaque to registry, e.g adding/encoding new feature does not involve registry
Experimental/Gradual Roll Out

- **Set in parent == live**
  - Clients will pick it up as TTL expires
  - Clients will also retain it until TTL expires
- **Mitigated by 1 new NS amongst existing pool**
  - Fine for most use case
  - Resolvers do a good job at finding a working NS
- **Does not work well for secured-protocols**
  - DNSSEC is either on or off for the whole domains
  - Secure-aware resolvers should not fallback to unsecured-protocols
  - Causes for service outages
  - Hinders adoption of secured-protocols