Use Case for Opportunistic Encryption for Recursive to Authoritative

Paul Hoffman

DPRIVE working group

IETF 108, virtual

2020-07-31

Use cases

- Resolver operator: “I’m happy to use encryption with the authoritative servers if it doesn’t slow down getting answers by much”
- Authoritative server: “I’m happy to use encryption with the recursive resolvers if it doesn’t cost me much”

Assumptions

- More encryption is good for the Internet
- Resolver vendors are smart and motivated
- Most resolvers don’t validate with DNSSEC and may never want to
- Authoritative operators don’t care much about encryption, but some would turn it on because more encryption is good for the Internet

It’s OK to have multiple use cases

- Use cases for draft-vandijk-dprive-ds-dot-signal-and-pin are always-secure encryption and no slowdown due to additional round trips
- Other sets of use cases may also be popular

Thoughts (not actual design)

- Recursive keeps a cache of what it knows about each authoritative's transport
- The cache can be pre-populated if there is a discovery mechanism
- Key can be IP addresses and/or domain names
- Like all caches, entries would time out
- Resolver vendors are creative and probably have their own thoughts

Actual design

- TBD
- You're probably thinking of one now
- The person after you in the queue is probably thinking of one that is different-but-similar or different-by-far
- The design is not as important as determining if this WG is interested in the use case