Statement on DNS Encryption

Root Server Operators
March 2021

The Root Server Operators are well aware of the active work taking place around DNS Encryption. The IETF's DPRIVE and DOH working groups have developed proposed standards for encrypted DNS between stub resolver and recursive resolvers. DNS-over-TLS is specified in RFCs 7858 and 8094, and DNS-over-HTTPS in RFC 8484. Also, currently under development is a protocol for DNS-over-QUIC.

Now that solutions and standards exist for encryption between stub resolvers and recursive resolvers, attention turns toward providing privacy protection for the next step: recursive resolvers to authoritative servers. A significant challenge here is agreement on the best way for authoritative servers to signal their support for and preferences regarding encrypted transports.

Due to the critical role that root name servers play, combined with the fact that they are themselves often targets of DDoS attacks, Root Server Operators have some concerns about supporting DNS encryption for serving the root zone. It is well known that UDP has desirable performance characteristics, due to its stateless nature. Increasing the state-holding burden with the addition of connection-oriented protocols, as well as encryption data, not only reduces the performance of name servers, but also may raise new types of denial-of-service attacks.

At this time, the exact risk-reward tradeoffs for deployment of encryption to root name servers is unclear and will likely depend on which particular transport proposals gain momentum. Root Server Operators do not feel comfortable being the early adopters of authoritative DNS encryption and would like to first see increased deployment in other parts of the DNS hierarchy. Meanwhile, there are other ways to improve privacy in queries sent to root and other name servers.

QNAME Minimisation (RFC 7816) is a technique that recursive resolvers use to send the shortest possible name to an authoritative server. In the context of the root zone, this means that recursive resolvers need only send the top-level domain (TLD) portion of a particular name. For example, rather than send a fully-qualified domain name like 'www.example.com', the recursive resolver can send a query for only 'com'.

Aggressive DNSSEC Caching (RFC 8198) is another privacy-enhancing technique. Under this protocol, a recursive resolver is able to use DNSSEC data from negative responses to cache the fact that no names exist between a certain range. Future requests can be answered from this cached data, rather than sending another query to an authoritative server. For example, when a recursive server learns that the root zone contains no names (TLDs) between '.coop' and '.corsica' then it can avoid sending queries for non-existent names such as 'mycompany.corp'.

Root Server Operators encourage the increased deployment of both QNAME minimisation and aggressive DNSSEC caching, which are available in recent releases of recursive DNS software. These features provide privacy benefits at all levels of the DNS and go a long way toward addressing privacy concerns of queries to the DNS root without the overhead of connection-level encryption.