Name Brian Dickson
Trip IETF 106
Trip Dates Nov 14-23 2019

Report Date Dec 2, 2019

1. **Describe the purpose(s) and outcome(s) of the trip in sufficient detail.**
    a. **Attend IETF 106**

2. **Describe the details of your attendance and activities, including sessions attended, presentations, or contributions made to specific sessions, etc.**
    a. **abcd BOF**
        i. **IMNSHO: Pretty much what was expected; not likely to reach solid consensus. Browsers will progress underlying tech regardless. Bad for DNS generally, especially bad for anyone using DNS in non-generic ways (RPZ, enterprise, UK, etc.) Bad for cross-app sync, scaling, info leakage, etc.**
    b. **dnsop**
        i. **Message Digest for zones (to validate data in XFR), pretty much done; 2-3 implementations, standards track**
        ii. **Extended DNS Errors (more codes/subcodes, plus text) – making good progress**
            1. **Main issues are: forwarders; truncation of text vs rest; TC or new bit;**
        iii. **Service Binding (WWW), aka SVCB/HTTPSSVC – very popular, bikeshed on names, early allocation soon**
            1. **Big contention areas are: CNAME/DNAME/Alias-form interop; chain length**
        iv. **Interoperable DNS Cookies – non-controversial, good progress**
        v. **DNS over TCP requirements – status, good**
        vi. **RDBD (related domains by DNS) – kind of early, needs work**
        vii. **DNSSEC validator ops recommendations – good work, progressing, but still a little early, lots of interest now**
        viii. **Avoid IP fragmentation – well motivated, needs more background/data, very useful/helpful; vs cookies, TCP?**
        ix. **User Assigned ISO 3166-1 (unused 2-byte codes for private use “TLDs”) – some disagreement but likely very useful and very probably will progress**
        x. **DNS Timeout RR (handle clean-up of dynamic updates that never go away) – probably progressing, not really controversial, mostly details(?); not actually presented/discussed (time out, meta/irony)**
    c. **Httpbis**

        i. Mostly irrelevant, except one MAJOR thing (IMNSHO, being “submarined” without DNSOP et al awareness):
            1. draft-ietf-httpbis-http2-secondary-certs
            2. Relies on previously published RFC 8336, which allows “no DNS lookup” for allegedly same server.
            3. New work is to link certs together (child->parent) to bypass DNS entirely, weakening DNS owner control, and relying ENTIRELY on revocation (CRL, OCSP, CT)
            4. This should be stomped on
            5. Previous RFC 8336 should be revised or nuked
            6. Oversteps bounds of WWW into space belonging to DNS, i.e. usurping DNS resolution protections against private key leakage and certificate misissuance.
    d. homenet
    e. tls
        i. Big thing is ESNI (encrypted Subject Name Indicator), has linkages to/from DNS, unclear impact(s)
            1. Lots of hand-wavy arguments about DoH, DNSSEC, cache poisoning, and things like “does not make the situation significantly worse”. Tries to suggest DoH as an alternative to DNSSEC for protection.
            2. ESNI records have no provenance or authenticity within them
    f. cfrg
    g. idr
        i. Nothing much new; relevance of RPKI (ROA validation) for BGP announcements, tangentially applicable to IP routes for DNS servers including root servers
    h. grow
        i. Route leak detection/mitigation; to be adopted by WG (I am co-author); should solve route leaks incrementally as deployed, especially at Tier-1 Networks.
        ii. Solves accidental leaks; analogous to projections against hijacks (which are solvable only by RPKI/ROAs)
    i. dprive
        i. Privacy considerations work
        ii. Recursive-to-authoritative work (requirements stage currently)
        iii. XFR over TLS (ongoing work)
        iv. Oblivious DNS over HTTPS (decouples IP and query, protects against resolver operator abuse, is a proxy model, has same weaknesses, too early currently)
        v. Privacy policy assertion (not ready for prime time, not well defined)
        vi. Adaptive DNS privacy (not well defined, too weak currently, lots of discussion)

vii. DNSSEC – GoDaddy to deploy signing availability for all customers (real soon now)

j. RSSAC Caucus meeting

3. Explain specific plans for follow-up activities in the RSSAC Caucus to enhance and continue the impact of the trip.

a. I plan on actively working on the following DNS-specific work:

b. DNS resolver identity, discovery, trust anchor, and encrypted transport drafts.

i. There is an overlap in needs between the dprive, dnsop, and abcd WGs, for methods to discover forwarder/resolver topologies, forwarder/resolver identities and addresses, the ability to establish trust anchors, and the ability to establish encrypted transport to actual resolvers (versus forwarders).

ii. Trust anchors allow for validated identity and parameter discovery (e.g. using DNSSEC signed records)

iii. Trust anchors facilitate certificate validation (e.g. using DANE TLSA types 2 and 3), required for encrypted transport and for validating resolver-specific functionality (such as RPZ responses)

iv. Topology discovery is an important feature lacking in the current deployment models of forwarders, e.g. “DNS traceroute”

v. DNS resolver selection for encrypted transport, requires determination of available resolvers and their respective capabilities and transports, availability, and performance characteristics

vi. Backwards compatibility is a requirement. Incremental deployment is a requirement. Topology discovery should maximize the actual topology including new and old forwarders/resolvers.

vii. Encrypted DNS transport to resolvers requires validation of the resolver identity, the topology, and the nature of the resolver.

viii. Stub client usage of forwarders/resolvers requires a means of transport encryption validation to the resolver.

ix. Encryption from resolver to authoritative requires additional means for confirmation of use of encrypted transport.