draft-wouters-edns-tcp-chain-query and draft-wouters-edns-tcp-keepalive

Paul Wouters
pwouters@redhat.com

Nov 5, 2013

draft-wouters-edns-tcp-chain-query-01

"Give me the A record of www.nohats.ca plus all supporting DNSSEC records for validation starting from ca's DNSKEY"

- Reduce wait time for DNSSEC validating on high latency links
- Avoid creating DNSSEC transports via HTTP GET
- Avoid creating DNSSEC transports via TLS X.509 extensions
- Avoid creating new DNS formats (JSON, XML, blobs)

- Avoid UDP amplification attacks - TCP or UDP with Eastland cookies

dig mock-up #1

```
; <<>> DiG 9.9.3-rl.13207.22-P2-MOCK_UP <<>> +dnssec +cq ca. www.nohats.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40959
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096; chain-query: ca.;
;; QUESTION SECTION:
;www.nohats.ca. IN A

;; AUTHORITY SECTION:
nohats.ca. 3425 IN DNSKEY 257 3 8 AwEAAZ5 [...]
nohats.ca. 3425 IN DNSKEY 256 3 8 AwEAAah [...]
nohats.ca. 3425 IN RRSIG DNSKEY 8 2 3600 20131111202444 20131028081233 18502 nohats.ca. I2G [...]
nohats.ca. 86242 IN DS 18502 8 2 DE760DB8D402E37F0AAB04CA04255DD6FFD850D386CB88423ED1520 6569EDF1
nohats.ca. 86242 IN RRSIG DS 8 2 86400 20131111172520 20131104172520 49200 ca. QJ14[...]

;; ANSWER SECTION:
www.nohats.ca. 3589 IN A 193.110.157.102
www.nohats.ca. 3589 IN RRSIG A 8 3 3600 20131115004440 20131101042553 21354 nohats.ca. jALhU [...]
```

dig mock-up #2

```
; <<>> DiG 9.9.3-rl.13207.22-P2-MOCK_UP <<>> +dnssec +cq ca. www.nohats.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40959
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 8, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096; chain-query: ca.;
;; QUESTION SECTION:
;www.nohats.ca. IN A

;; AUTHORITY SECTION:
nohats.ca. 3425 IN DNSKEY 257 3 8 AwEAAZ5 [...]
nohats.ca. 3425 IN DNSKEY 256 3 8 AwEAAah [...]
nohats.ca. 3425 IN RRSIG DNSKEY 8 2 3600 20131111202444 20131028081233 18502 nohats.ca. I2G [...]
nohats.ca. 86242 IN DS 18502 8 2 DE760DB8D402E37F0AAB04CA04255DD6FFD850D386CB88423ED1520 6569EDF1
nohats.ca. 86242 IN RRSIG DS 8 2 86400 20131111172520 20131104172520 49200 ca. QJ14[...]
--> nohats.ca. 3533 IN NS ns0.nohats.ca.
--> nohats.ca. 3533 IN NS ns1.nohats.ca.
--> nohats.ca. 3089 IN RRSIG NS 8 2 3600 20131114090125 20131031082553 21354 nohats.ca. aI17[..]

;; ANSWER SECTION:
www.nohats.ca. 3589 IN A 193.110.157.102
www.nohats.ca. 3589 IN RRSIG A 8 3 3600 20131115004440 20131101042553 21354 nohats.ca. jALhU [...]

;; ADDITIONAL SECTION:
--> ns0.nohats.ca. 3600 IN A 193.110.157.102
--> ns0.nohats.ca. 2744 IN RRSIG A 8 3 3600 20131117220110 20131103213849 21354 nohats.ca. RiR[...]
--> ns1.nohats.ca. 3600 IN A 66.160.143.188
--> ns1.nohats.ca. 2682 IN RRSIG A 8 3 3600 20131115200836 20131101182458 21354 nohats.ca. AMgO[..]
```

draft-wouters-edns-tcp-chain-query

- Does this in fact speed up DNS on high latency mobile networks?
- What is the impact of additional TCP on upstream recursive nameservers?
- Positive response for implementation by Bind and Unbound
- Should NS records and glue be included?

draft-wouters-edns-tcp-keepalive

- Goal #1: Advertise TCP can be used for more than 1 query
- Goal #2: Advertise a timeout value for (idle?) TCP session.
- Measurements:
  - Used a patched dig (thanks Mark Andrews!)
  - Scripted a few hundred queries against DNS resolvers
  - Current versions of bind, unbound, powerdns-recursor and dnsmasq work fine
  - OpenDNS worked fine
  - Google DNS closes TCP after 64 queries
- Conclusion:
  - #1 seems not needed. Some concern new EDNS options break existing implementations
  - #2 is this worth an EDNS option by itself?