

DNSSEC Roadblock Avoidance

Status, Next Steps

Has Running Code (multiple versions)

Does it have Rough Consensus?

One outstanding item from authors:

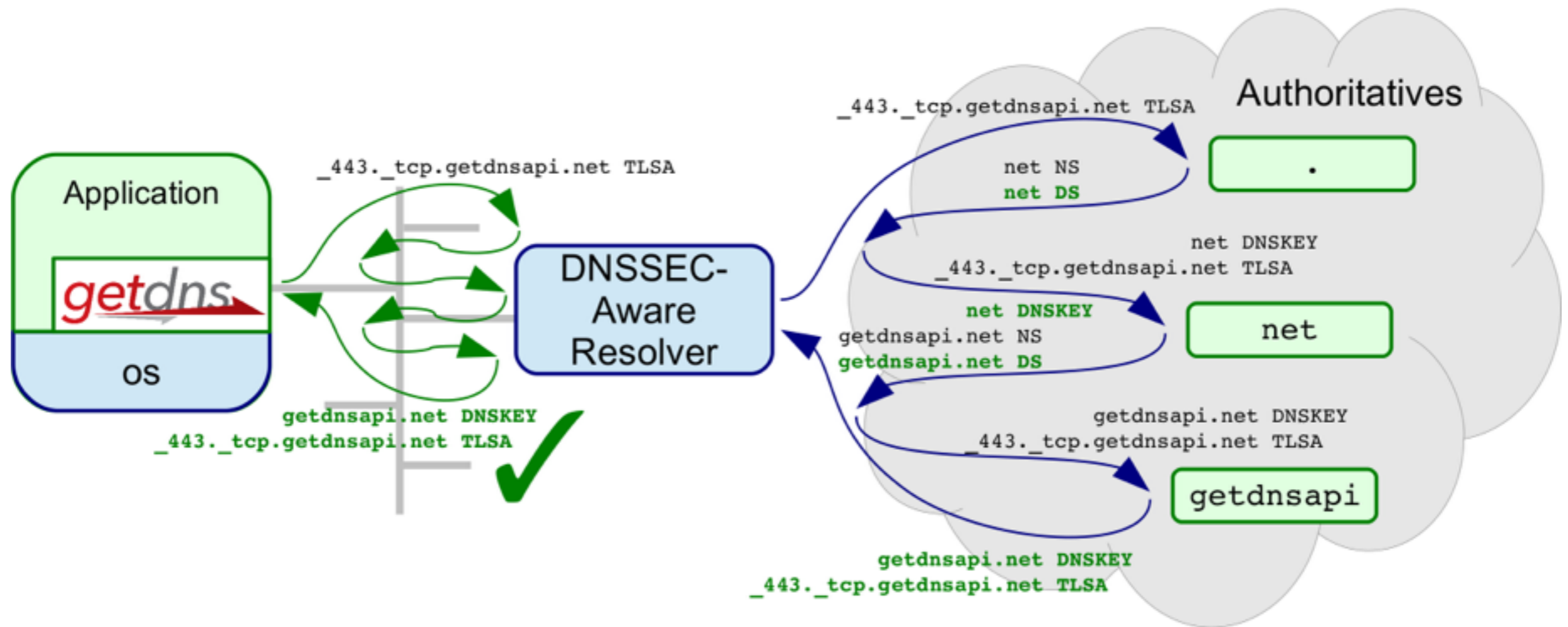
(from 1 July)

We explicitly punt on explaining how to overcome the situation when a ‘proxy/forwarder’ “randomly” sends queries to Resolvers with different capabilities.

(Petr’s words w/out the IPR baggage?)

Running Code Example

Willem Toorop/Benno Overeinder - DNSSEC Roadblock Avoidance



The recursive resolver needs to be DNSSEC-Aware
There are many middle boxes and others that are not.
[draft-ietf-dnsop-dnssec-roadblock-avoidance](#)

Results for 208.67.222.222:

Query for alg-8-nsec3.dnssec-test.org returned answers: 1
Query for alg-8-nsec3.dnssec-test.org did not have an secure answer: 1
Query for realy-doesnotexist.dnssec-test.org. did not return answers: 2
Query for realy-doesnotexist.dnssec-test.org. was not secure: 2
Query for dnssec-failed.org returned answers: 2
rcode for dnssec-failed.org was not SERVFAIL: 2
Query for alg-13-nsec3.dnssec-test.org returned answers: 3
Query for alg-13-nsec3.dnssec-test.org did not have an secure answer: 3

dnssec data
for answers

dnssec data
for non existence



Also try:

DNS Advantage	156.154.70.1	156.154.71.1
Dyn Internet Guide	216.146.35.35	216.146.36.36
Google	8.8.8.8	8.8.4.4
Level 3	209.244.0.3	209.244.0.4
OpenDNS Home	208.67.222.222	208.67.220.220
Verisign	64.6.64.6	64.6.65.6

Roadblock

```
willem@bonobo: ~/repos/getdns/src/test 107x10
$ ./getdns_query -s 208.67.222.222 _443._tcp.getdnsapi.net TLSA +dnssec_return_only_secure
SYNC response:
{
  "answer_type": GETDNS_NAMETYPE_DNS,
  "replies_full": [],
  "replies_tree": [],
  "status": GETDNS_RESPSTATUS_ALL_BOGUS_ANSWERS
}
$

root@bonobo: ~ 107x19
root@bonobo:~# tcpdump -n -i wlan0 port 53
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:37:26.472680 IP 133.93.33.101.52794 > 133.93.5.6.53: 12289+% [1au] Type52? _443._tcp.getdnsapi.net. (52)
13:37:26.480307 IP 133.93.5.6.53 > 133.93.33.101.52794: 12289 3/4/9 Type52, Type52, RRSIG (1053)
13:37:26.480408 IP 133.93.33.101.49994 > 133.93.5.6.53: 54826+% [1au] DNSKEY? . (28)
13:37:26.480448 IP 133.93.33.101.59537 > 133.93.5.6.53: 9457+% [1au] DNSKEY? getdnsapi.net. (42)
13:37:26.480462 IP 133.93.33.101.35434 > 133.93.5.6.53: 18876+% [1au] DS? getdnsapi.net. (42)
13:37:26.491535 IP 133.93.5.6.53 > 133.93.33.101.49994: 54826$ 3/0/1 DNSKEY, DNSKEY, RRSIG (736)
13:37:26.491593 IP 133.93.5.6.53 > 133.93.33.101.59537: 9457$ 3/0/1 DNSKEY, DNSKEY, RRSIG (767)
13:37:26.493733 IP 133.93.5.6.53 > 133.93.33.101.35434: 18876$ 2/0/1 DS, RRSIG (241)
13:37:26.493867 IP 133.93.33.101.41289 > 133.93.5.6.53: 9629+% [1au] DNSKEY? net. (32)
13:37:26.493898 IP 133.93.33.101.47624 > 133.93.5.6.53: 56937+% [1au] DS? net. (32)
13:37:26.496656 IP 133.93.5.6.53 > 133.93.33.101.41289: 9629$ 3/0/1 DNSKEY, DNSKEY, RRSIG (743)
13:37:26.497810 IP 133.93.5.6.53 > 133.93.33.101.47624: 56937$ 2/0/1 DS, RRSIG (239)
```