Measuring Efficiency of Aggressive Use of DNSSEC-Validated Cache (RFC 8198)

Was it worth the effort?

Petr Špaček • petr.spacek@nic.cz • 2018-03-08
Talk outline

- RFC 8198 promises
- Normal traffic
- Random subdomain attack
RFC 8198: Promises

- Use of NSEC/NSEC3 RRs to
  - increase "performance"
  - decrease latency
  - decrease resource utilization
  - increase privacy
  - increase resilience
RFC 8198: Efficiency

- Query pattern
  - normal traffic
  - random subdomain attack
- Distribution of names in DNS zones
- Wildcards
- TTL
RFC 8198 + NSEC vs. Normal traffic
Normal traffic: Experimental setup

- Replay query PCAP to BIND 9.12.0
  - synth-from-dnssec yes / no;
- Record to PCAP
  - traffic to auth
  - answers
- Analyze
  - # packets to auth
  - bandwidth to auth
  - latency for answers
Normal traffic: Data set

- 2 hours of traffic in PCAP
- Public Open Resolver run by CZ.NIC
  - ~ 2500 q/second (excluding QTYPE=ANY)
  - 14 % answers NXDOMAIN
  - 3 % answers SERVFAIL
  - anonymized
Normal traffic: Tools

- BIND 9.12.0
  - "unlimited" cache size (max-cache-size unlimited)
- Drool 1.1.0 to replay traffic with timing
- DNS Collector to analyze latencies
  - (new project by CZ.NIC, to be released)
- Libtrace 3.0.21 to analyze packet #, bandwidth
Normal traffic: Latency ... ?

BIND 9.12.0 Response Time

- synth-from-dnssec yes;
- synth-from-dnssec no;

Response time [ms] vs. Slowest percentile.
RFC 8198's promises & normal traffic

- Lower latency
  - Some unexplained increase, a measurement error?
  - Likely not significant for eyeballs (0.1 vs 10 ms)
- Lower network utilization
  - Small but reproducible decrease
  - 1-2 % decrease of # packets to auth
  - 3-4 % decrease of bandwidth to auth
RFC 8198 + NSEC
VS.
Random subdomain attack
R.S.A. traffic: Experimental setup

- Auth server with a test zone
- Replay random query names to Knot Resolver
- Record traffic to auth into PCAP
- Analyze
  - # packets to auth
  - bandwidth to auth
R.S.A. traffic: Tools

- Knot DNS 2.6.4
  - RSASHA256 2048 b, automatic signing
- Knot Resolver 2.1.1
  - "unlimited" cache size (20 GiB)
- dnsperf 2.1.0 to replay queries
- libtrace 3.0.21 to analyze packet #, bandwidth
R.S.A. traffic: Query pattern

- 1000 simulated clients
- Next query right after answer to previous query
- Pseudorandom unique query names (256 bits)
  - GCZDKQIS7F7THXBIIBC4HHZDYTFCPH5XLR6PGEI3WIESK7BS45WQ.test.knot-resolver.cz. A
  - GCZDKQIS7F7THXBIIBC4HHZDYTFCPH5XLR6PGEI3WIESK7BS45WQ.test.knot-resolver.cz. AAAA
  - OF6OVT2SNIV54B7HI77V5TJ3TFVULN5AMQ2Z6IWQX6GBHQ254LNQ.test.knot-resolver.cz. A
R.S.A. scenarios

- Unsigned zone (baseline)
- Signed zone
  - SOA minimum, NSEC TTL
    - 3600 s / 60 s
  - name distribution (real zones)
    - small zone with wildcard (50 names + 1 wildcard)
    - medium size zone (14k names)
    - big zone (110k names)
    - huge zone (1M names)
R.S.A.: unsigned zone (abs baseline)

Cache size: 19.2 GB

- Traffic to auth [packets per second]
- Traffic to auth [MiB/s]

- Packets to auth
- Bandwidth to auth

Time from beginning of the attack [minutes]
R.S.A.: unsigned zone (baseline %)

- Cache size: 100%

Graph showing packets to auth and bandwidth to auth over time from the beginning of the attack in minutes.
R.S.A.: 50 names + wildcard, TTL 60

Cache size: 0.0006 %
R.S.A.: 14k names, TTL 3600

- packets to auth
- bandwidth to auth

Cache size: 0.004%
R.S.A.: 110k names, TTL 3600

The graph shows the decrease in packets to auth and bandwidth to auth over time from the beginning of the attack. The cache size is 0.13%. The y-axis represents the percentage of packets/s to unsigned zone, while the x-axis represents the time from the beginning of the attack in seconds.
R.S.A.: 110k names, TTL 3600
R.S.A.: 110k names, TTL 3600

Packets to auth
Badwidth to auth

Cache size: 0.13 %

Time from beginning of the attack [minutes]

Packets to auth [% of packets/s to unsigned zone]
Bandwidth to auth [% of MiB/s to unsigned zone]
R.S.A.: 1M names, TTL 3600

The graph shows the percentage of packets to auth and bandwidth to auth as a function of time from the beginning of the attack. The cache size is 0.56%.
R.S.A.: 1M names, TTL 3600

![Graph showing packets to auth and bandwidth to auth over time from beginning of the attack.
Cache size: 0.56%]
R.S.A.: 1M names, TTL 3600

cache size: 0.56 %
R.S.A.: 1M names, TTL 3600

cache size: 0.56 %
R.S.A.: 1M names, TTL 60

cache size: 0.53 %

The graph shows the number of packets and bandwidth to the auth server over time from the beginning of the attack. The red line represents packets to auth, and the blue line represents bandwidth to auth.
R.S.A.: 1M names, TTL 60

![Graph showing packet and bandwidth distribution over time with cache size 0.53%](image-url)
RFC 8198's promises & R.S.A. traffic

- ✔ Much better cache usage
- ✔ Significantly lower network utilization
  - Eliminates R.S.A. traffic (over time)
Was RFC 8198 worth the trouble?

- **YES!** (if you use NSEC)

- Normal traffic
  - NSEC only → not a significant difference ??

- Random subdomain attack
  - small & medium zones → eliminates traffic
  - big & huge zones w/ long TTL → eliminates traffic
  - big & huge zones w/ short TTL → cuts traffic to 10-40%

- NSEC 3 & algorithm impact to be investigated
Knot news for spring 2018

- Knot DNS 2.7
- Performance optimizations
- Security audit
- DNS cookies

- Knot Resolver 3.0
- NSEC 3 support for aggressive cache
- Cache pre-fill mechanism