deSEC

nlnet FOUNDATION

2022-04-063: Post-Quantum Crypto in DNSSEC

Report on Milestones 3.a–c

Milestone 3 of 2022-04-063 (Post-Quantum Crypto in DNSSEC) does not entail production and publication of code, but rather designing, performing, and analyzing field measurements using the implementations from Milestones 1 (PowerDNS) and 2 (BIND). This report is to provide documentation / evidence as to the completion of the tasks in this milestone.

Milestone 3.a: Study Design

The purpose of the project is to explore DNSSEC in the context of post-quantum cryptography, especially with regards to transport and deliverability issues caused by larger-than-conventional keys and signatures. This milestone is about defining how exactly to execute the field study.

Methodology

We first evaluated a number methodologies, taking into account the goal of covering a large, global population of vantage points. (Uniformity is not necessarily required as results can be weighted by vantage point density per country, if needed.) Further criteria included low noise, direct measurement (as opposed to indirect), and cost. We assessed the following approaches:

- **RIPE ATLAS** (community-run measurement platform with lots of small probe devices)
  - **pro:** >10,000 vantages points; credit-based, with some number of credits available to deSEC every month; well-documented; DNS queries can be performed directly
  - **con:** noisy (~10%); uncertain population characteristics
- **Thousand Eyes** (commercial measurement platform)
  - **pro:** little noise, according to other users
  - **con:** indirect measurement (only HTTP queries, from whose success DNS behavior needs to be inferred); no public pricing available; uncertain population characteristics
- **Ad-based** (run JavaScript through ads on web pages)
  - **pro:** very comprehensive sample
  - **con:** indirect measurement (HTTP only); must organize measurements as a request sequence, which might abort (e.g., user closes tab / navigates to different page); costly
- **SMTP-based** (send email and inspect DNS queries resulting from recipient server performing anti-spam measures like “sender verify”)
  - **pro:** allows view from within enterprise internal networks
  - **con:** duplication of results from high concentration around cloud email providers expected (Outlook, GMail, …); inefficient / would need to send lots of unsuccessful trial-and-error email (not all email operators perform the DNS queries of interest); correlation of DNS queries with “sender verify” might be not be a safe assumption; high noise expected (from unknown/unrelated failure modes)

We were surprised that direct DNS measurements were only supported by RIPE ATLAS. (We expected dedicated measurement platforms such as Thousand Eyes to support that, too.) One drawback of RIPE ATLAS is its comparably high noise level (as in, meaningless DNS answers from broken setups), but quick experiments showed that it can be controlled using pre-classification of vantage points (“probes”) based on whether non-PQC queries give reasonable results.

We decided to proceed with RIPE ATLAS, but include additional anti-noise variables in our measurements, to be used as a cross-check on each probe's suitability for inclusion in the final measurement sample (see below). As far as cost is concerned, DNS queries cost 10 or 20 credits, via UDP and TCP, respectively.

Both the noise control variables as well as our decision to add more PQC algorithms than initially envisioned, quickly led us to realize that several million credits would be needed, as deSEC's monthly 1M quota, corresponding to ~67k queries, would be insufficient. Luckily, the community turned out very friendly, and we were able to quickly gather the necessary amount of credits by means of donation (transfer into our account).

Observables

We were interested in measuring DNS lookup success in the presence of PQC DNSSEC configurations, and determined the following variables to be of interest:

- **Rcode:** DNS response code (NOERROR, NXDOMAIN, SERVFAIL, REFUSED, FORMERR)
- **Correctness:** Whether the response content was correct
- **AD bit:** Whether the probe's resolver indicated that the response was DNSSEC-validated (expected only for conventional algorithms)
- **Response time**

We set out to investigate these four quantities along several dimensions, namely

1. The **PQC algorithm** used (Falcon-512, Dilithium2, SPHINCS+, XMSS)
    - For **noise control**, we added unsigned (non-DNSSEC) test cases as well as conventional DNSSEC scenarios (algorithms 8, 13, and 15)
2. **Vendor:** Measurements were done with both PowerDNS and BIND implementations.
3. **Existence:** Whether the name in the query existed or not
    1. For existing names, we queried an A record and considered the response *correct* if the *rcode* was NOERROR and the response content contained the expected IP address
    2. For non-existing names (a subdomain without records), we considered the answer *correct* if the *rcode* was NXDOMAIN
4. **NSEC(3):** For negative responses (non-existing names), we prepared an NSEC and an NSEC3 scenario, corresponding to different types of DNSSEC "denial of existence" proofs.
    - NSEC3 comes in several flavors; we used "narrow" mode for PowerDNS, and "non-narrow" for BIND. The different flavors cause different response size.
5. **Transport:** UDP vs. TCP
6. **DO bit:** Some resolvers do not retrieve DNSSEC records if the client does not set the DO bit. To investigate these effects, we conducted measurements for both cases (set vs. unset).
7. **Key setup.** We used a KSK/ZSK split setup for BIND, and CSK with PowerDNS.
    - DNSSEC keys are typically set up in one of two ways: (1) a split-key setup, where one key is used for entry into a zone ("key-signing key", KSK) and another key is used to sign the rest of the zone ("zone-signing key", ZSK); (2) a single key is used ("combined signing key", CSK). This mainly affects response size for queries of type DNSKEY.

Combining all of the above multiplies quickly, resulting in a large set of configurations, which in turn allows a comprehensive view on the state of DNS resolution depending on the various parameters.

We did not distinguish queries via IPv4 and IPv6. This is because probes make queries to their local resolvers, which in turn query our authoritative nameservers. RIPE ATLAS only controls the first part (between probe and resolver), but the crucial traffic actually flows through the other part (between resolver and nameserver). Parameterizing queries through RIPE ATLAS thus would not have enabled any new conclusions. For simplicity, we then ran our nameservers on IPv4 only.

Impact of IP address family behind the resolver could have been investigated by duplicating deployments, with nameservers of half the zones reachable only via IPv4, the other half via IPv6. Apart from the additional testing needed, this would have doubled the cost (4 VMs instead of 2, and twice as many measurements). However, compared to other effects, the impact is expected to be small: DNS message deliverability mostly depends on response size, which in our study is dominated by PQC signature and key sizes; an IPv6 header being a little larger than an IPv4 header would barely make a difference. Indeed, meaningful conclusions were drawn even without this dimension. Also facing RIPE ATLAS quota limitations (see below), adding it seemed neither practical nor justified.

Milestone 3.b: Field Study

Before performing measurements, the above study design required extending the test bench setups (milestones 1.b, 2.b) to enable noise control (by adding unsigned / conventionally signed zones). Once that was done, we performed small test measurements with RIPE ATLAS, and then proceeded to full measurements. Overall, we spent 67.5M credits (corresponding to 4.5M queries).

Logistics were somewhat complicated, as there is a limit to the number of measurements that can be submitted in a batch. This was solved by using multiple batches. In addition to this technical limit, we also encountered various quotas, such as how many measurements can be pending at a given time, how many results can be generated per day, etc. (We should have anticipated those ...)

Due to the quotas, measurements were projected to take three to six weeks. This was a problem, because in case of an issue, a whole month would be lost. Interacting with RIPE ATLAS administrators, we were able to set up scheduling schemes that allowed us to proceed more quickly, without unduly burdening any single probe or the central systems.

RIPE ATLAS measurement results are public and made available here (in raw format): https://atlas.ripe.net/measurements/public?id__gt=1000000&is_public=true&sort=-id&toggle=all&page_size=100&search=pq-dnssec.dedyn.io&page=1

Milestone 3.c: Processing / Analyzing Results

After collecting measurement results, we processed them into CSV format and made them available at: https://pq-dnssec.dedyn.io/results.csv

We then performed analysis, using the following pre-selection:

- Exclude probe-resolver combinations that did not give a correct response for conventional RSA-SHA256 (algorithm 8). Note that unvalidated responses with otherwise correct attributes were not excluded. (The purpose of the filter is not to enforce DNSSEC, but to remove responses from entirely broken probes.) This reduced the noise level significantly.
- Exclude resolvers from private IP ranges (such as 10.0.0.0/8). The reason for this is that due to a technical limitation, RIPE ATLAS is not able to query these IP ranges via TCP. (We learned this along the way by observing errors, and then inquired with RIPE ATLAS.) To keep things comparable, we applied the same constraint to UDP. This reduced sample size somewhat, but not in a problematic way.

Insights and code of the analysis can be seen in our presentations and other public updates (milestones 3.d and 4).

Peter Thomassen, July 2024