Extended Error Reporting

Reporting errors to where it may be fixed

Roy Arends
Principal Research Scientist, ICANN's Office of the CTO

13 October 2022

How it started

आ **Anand Buddhdev**
@aabdnn

.UK ZSK rollover appears to have gone wrong, and we need to restart caches to flush out the old ZSK :(#fail #dnssec

8:25 PM · Sep 11, 2010 · Twitter Web Client

Introduction

- Friday, September 10th, 2010 19:38:11
  - The main DNSSEC signing system suffered a kernel panic
  - Failover to the secondary system lead to a signed zone with an old ZSK
  - Validates fine, since the chain of trust was completely intact
  - Unless you use a previously cached keyset, which had a different (newer) ZSK
  - Failure reports on twitter alerted Nominet about the issue

The problem

- DNS problems are not obvious to the end user
- DNS problems observed at a resolver do not automatically get reported to the domain holder
- Real world, risk free testing with DNSSEC deployment is not possible.

First problem

- DNS failures are not obvious. It often manifests in the form of
  - The Internet is offline!!1!!one?!
  - Or “SERVFAIL” at best
- SERVFAIL hides
  - Lame delegations, DNSSEC validation failures, etc
- This lead to the creation of RFC8914
  - Extended DNS Errors

RFC 8914 (October 2020)

Method to return additional information about the cause of DNS errors.

```
$ dig @1.1.1.1 dnssec-failed.org
; <<>> DiG 9 <<>> @1.1.1.1 dnssec-failed.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 41151
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; EDE: 9 (DNSKEY Missing): (no SEP matching the DS found for dnssec-failed.org.)

;; QUESTION SECTION:
;dnssec-failed.org.      IN   A

;; Query time: 1 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; MSG SIZE  rcvd: 103
```

RFC 8914 (October 2020)

INFO-CODE	Purpose	Reference
0	Other Error	[RFC8914, Section 4.1]
1	Unsupported DNSKEY Algorithm	[RFC8914, Section 4.2]
2	Unsupported DS Digest Type	[RFC8914, Section 4.3]
3	Stale Answer	[RFC8914, Section 4.4][RFC8767]
4	Forged Answer	[RFC8914, Section 4.5]
5	DNSSEC Indeterminate	[RFC8914, Section 4.6]
6	DNSSEC Bogus	[RFC8914, Section 4.7]
7	Signature Expired	[RFC8914, Section 4.8]
8	Signature Not Yet Valid	[RFC8914, Section 4.9]
9	DNSKEY Missing	[RFC8914, Section 4.10]
10	RRSIGs Missing	[RFC8914, Section 4.11]
11	No Zone Key Bit Set	[RFC8914, Section 4.12]
12	NSEC Missing	[RFC8914, Section 4.13]
13	Cached Error	[RFC8914, Section 4.14]
14	Not Ready	[RFC8914, Section 4.15]
15	Blocked	[RFC8914, Section 4.16]
16	Censored	[RFC8914, Section 4.17]
17	Filtered	[RFC8914, Section 4.18]
18	Prohibited	[RFC8914, Section 4.19]
19	Stale NXDomain Answer	[RFC8914, Section 4.20]
20	Not Authoritative	[RFC8914, Section 4.21]
21	Not Supported	[RFC8914, Section 4.22]
22	No Reachable Authority	[RFC8914, Section 4.23]
23	Network Error	[RFC8914, Section 4.24]
24	Invalid Data	[RFC8914, Section 4.25]
25	Signature Expired before Valid	[https://github.com/NLnetLabs/unbound/pull/604#discussion_r802678343][Willem_Toorop]
26	Too Early	[RFC9250]
27	Unsupported NSEC3 Iterations Value	[RFC9276]
28-49151	Unassigned	
49152-65535	Reserved for Private Use	[RFC8914, Section 5.2]

Second problem

- Failures do not automatically reach the place where they can be fixed
- Solution is straightforward:
  - Domain owner publishes a place where to report errors
  - Resolver sends error report to domain owner
- Similar to what DMARC does for SPF/DKIM for mail.

DNS-Error Reporting draft
draft-ietf-dnsop-dns-error-reporting

- Describes a method that lets resolvers signal errors back to the owner of a domain.
- The intent is to help domain owners and authoritative server operators detect misconfigurations earlier.
- Recent errors are a good example of the issues that can be reported
  - Failures due to DS records with different digests.
  - NSEC3 iterations higher than RFC5155 recommended CAP
  - DNSSEC configuration issues:
    - .beauty, .llp, .unicom, .firestone, etc etc
    - cdc.gov, caltech.edu, time.nist.gov, etc etc

How does it work?

- Authoritative server adds EDNS0 option to every response, containing a reporting agent domain, say “reporting-agent.example”
- When there is an error, the resolver prepends the extended error code (as a label) and the query type to the erroneous qname, and encapsulates it with an _er label:
  - Example: _er.7.1.broken.test._er
- Resolver appends the reporting agent domain to the erroneous qname.
  - Example: _er.7.1.broken.test._er.reporting-agent.example
- Resolver sends the query, which will end up at the reporting agent domain.
- The response can be nicely cached to avoid too many queries.

How is it going?

- This draft was first communicated to several DNS software development teams to get early feedback, which was overall positive.
- IETF hackathon resulted in a server-side implementation. The resolver-side depends on Extended DNS Errors (RFC8914) implementation and is in various dev. stages in resolvers.
- The DPRIVE Working Group has proposed using DNS records for discovery of whether an authoritative server offers DNS over encrypted transport.
- In such an environment, it would be useful for a resolver to be able to report to an authoritative server if such discovery records are in error.

The third problem

- Real world, risk free testing with DNSSEC deployment is not possible.
  - A lab environment is not the real world.
  - Using a different domain name for testing won't be used the same as your domain.
  - Environments change
  - Cryptographic Algorithms evolve
  - Keys need to be rolled

- What if?

Risk free, near real world testing

- Dry-run DNSSEC is a method whereby
  - All normal DNSSEC processing happens,
  - Except, in a case of an error, no servfail, just pretend DNSSEC was off, i.e. no impact to the user.
  - Error reporting, using the previously discussed method, will show if DNSSEC deployment will be successful.
  - This is the idea that is currently proposed in draft-yorgos-dnsop-dry-run-dnssec
    - Signalling dry-run-dnssec is still being discussed.

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: roy.arends@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg