Discovery method for a DNSSEC validating stub resolver

Xavier Torrent Gorjón
Supervisor: Willem Toorop

System and Network Engineering
Universiteit van Amsterdam

Research Project 2

Outline

Motivation

Insert motivational quote here.

Engineering Motto #1 : Live the present

If it works, do not change it.

Engineering Motto #2 : Life is unfair

When things work you never get a *"thank you"*. When things do not work, you better run for your life...

Motivation

The DNSSEC chain of ~~trust~~ blame.

1. NASA.GOV "blocked" by Comcast when implementing DNSSEC[1] (2012).
2. .GOV zones not resolving due errors in the DNSSEC configuration[2] (2014).
3. HBO NOW blocked due invalid signature at their servers[3] (2015).

Change creates problems...

...and users tend to blame the Internet Service Providers, which makes them reluctant of adopting "new" standards. Which makes legacy prevail. And we were told that was bad?

[1] `http://bit.ly/1GOrHxR`
[2] `http://bit.ly/1gbP7aP`
[3] `http://bit.ly/1GoasVi`

Motivation

Buying cheap is expensive. . .

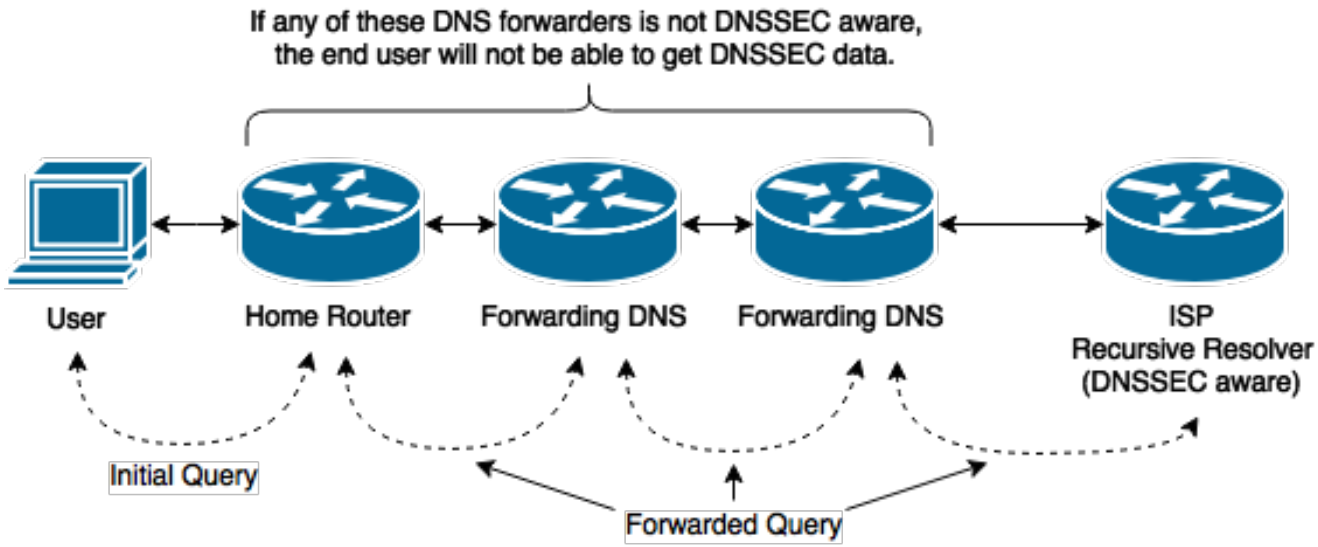


Figure: DNSSEC may be "blocked" by DNS forwarders, or the home router.

Research Question

- How can a stub resolver use a discovery method to process data from a recursive resolver?

Related Work

OS3 likes DNS.

- **DNSsec Revisited** RP 2014, *Anastasios Poulidis, Hoda Rohani*
- **Measuring the deployment of DNSSEC over the Internet** RP 2014, *Nicolas Canceill*
- **DNSSEC deployment maps**
  `http://www.internetsociety.org/deploy360/dnssec/maps/`
- **RFCs** 1035, 2671, 4033, 4034, 4035, 5155.

Approach
Research HOWTO

- **Measure DNSSEC security aware resolvers** This part of the research has been done by using RIPE ATLAS.
- **Define a course of action for a stub resolver** Try to maintain as much scalability (shared cache) as possible.

Tools used

Ubuntu 15.04, Python 2.7.9, Python DPKT library, RIPE ATLAS. Special mention to the 'atlas' python class, courtesy of NLnet.

Approach

Research HOWTO

RIPE ATLAS

RIPE ATLAS is an online tool that can be used to query probes spread worldwide (mostly Europe) to get diverse measurements.

Designing the Measurements

Decisions, decisions. . .

We performed four different types of measurements:

- **Basic DNS.**
- **Basic DNSSEC.**
- **NXDOMAIN Handling test.**
- **Wildcard Handling test.**

NXDOMAIN

NXDOMAIN answers are –supposed to be– obtained when querying for a non-existant name.

Wildcards

DNS wildcard records are used to match any name that is not defined and is matched by the wildcard.

Filtering results

"Do *it right* or do not, there is no try."

Public DNS

We filtered the probes using public DNS servers as their resolvers, as this would likely inflate numbers.

Loopback addresses

A number of probes were using a loopback address (**127.0.0.1**) as their resolver.

Measurement Results: NXDOMAIN Handling (NSEC)

Not that promising...

Received Resource Records	Percentage
No RR	22.27%
Only SOA	21.49%
SOA + NSEC + RSIG(x2)	*56.23%*

- Over 10.000 measurements.

Measurement Results: NXDOMAIN Handling (NSEC3)

NSEC3 shares a similar fate.

Received Resource Records	**Percentage**
No RR	12.44%
Only SOA	27.68%
SOA + RRSIG	3.62%
SOA + NSEC3(x3) + RSIG(x3)	0.58%
SOA + NSEC3(x4) + RSIG(x3)	*57.86%*

- Over 10.000 measurements.

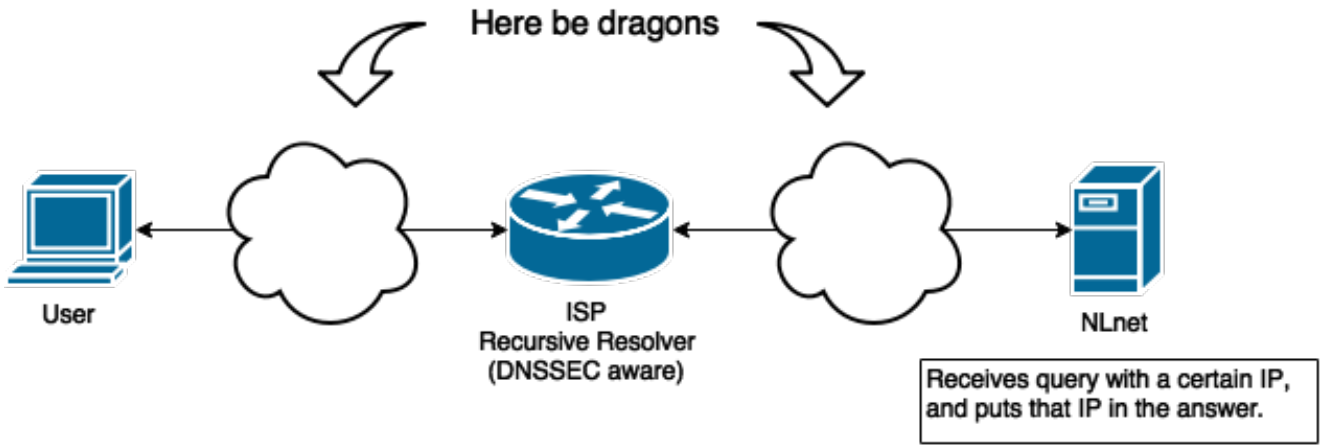
Measurement Results: Wildcard Handling

"Never tell me the odds."

Received Resource Records	Percentage
No RR	31.59%
NSEC + RRSIG	11.92%
NS(x3)	6.93%
NS(x3) + RRSIG	13.48%
NS(x3) + RRSIG + NSEC	1.10%
NS(x3) + RRSIG(x2) + NSEC	*34.98%*

- Over 10.000 measurements.

Forcing communication with ISP Resolver



Getting the address

Query for an A record to **echo.v4.nlnetlabs.nl.** Server does not reply a fixed record, but replies with the IP of the recursive resolver!

The results...

Querying directly the recursive resolver increased the DNSSEC query success to 80%!

Discovery Method

"Are we there yet? Are we there yet?"

1. **Primary DNS server:** Working 56% of the time for NXDOMAIN and 35% for wildcards.
2. **Secondary DNS server:** Tends to not be useful unless the secondary is set to be from a different 'provider'.
3. **Directly access ISP DNS server:** Our measurements indicate that this would rise success chance to approximately 80% (if ISPs do not block this).
4. **Use a public DNS server:** p.e. Google public DNS resolvers can process DNSSEC queries.
5. **Full recursion from stub resolver**

Conclusions

- DNSSEC is still not properly implemented, at a resolver level, in most –cheap– hardware.
- Errors are difficult to troubleshoot as they may originate at different points of the DNS communication.
- Querying directly the ISP resolver helps the issue.

Future Work

But wait, there is more. . . !

- It would be interesting to use an alternative method, rather than RIPE ATLAS, to determine the validity of the data we gathered.
- The dataset retrieved from RIPE could be studied in more depth than what 2 weeks of RP allow for. . .
- About the Checking Disabled bit. . .

Future Work

Future as in. . . *next week*.

Subject **Re: Feature request: set CD bit on atlas DNS measurements**

To Willem Toorop, Me <xavier.torrentgorjon@os3.nl>

Cc Robert Kisteleki <robert@ripe.net>, Philip Homburg <philip.homburg@ripe.net>,

```
Dear Willem,

As of today you can include the following parameter in the JSON definition:

"cd": true

This isn't officially documented yet, but once it is working for you I
will also document it and we will consider adding it to the web UI.

Kind regards,
Chris
```

Questions