PROFILING RESOLVERS

A CAUTIONARY TALE

Olafur Gudmundsson
Bob Novas
Shinkuro
ogud, bob.novas @ shinkuro.com

BACKGROUND

- "State-of-the-art" in DNS resolvers?
- Are there "sticky" resolvers out there?
- How "good" are resolvers?
- Moving validation to edge possible ?
- Measure "progress"

FCC WG

- FCC in US chartered a DNS working group to promote improvements in DNS service by ISP's
  - How to measure the quality of DNS service?

First Attempt

- Type
  - Not a resolver
  - RFC103x only
  - Pre-DNSSEC
  - DNSSEC aware
  - Validator
- Grade
  - F
  - D
  - C
  - B
  - A

GRADING TESTS

- F ->D: (1 test)
  - Answers a query for SOA
- D -> C (4 tests -> 5 results)
  - EDNS0, Unknown RR, TCP and DNAME supported
- C ->B (6 tests -> 6 results)
  - Returns Big (2K RRset) , DS, DNSKEY, DNAME, NSEC and NSE3 w. RRSIG
- B-> A (1 additional test -> 1 result)
  - Prior answers validate and it rejects a badly signed answer

GRADING PROBLEMS:

- Grades are easy to understand BUT ONLY those getting perfect score like being graded.
  - TCP disabled by policy -> D
  - DNAME not supported -> D
- Conclusion: grading is too harsh to be useful

DESCRIPTIVE RESULTS

- Old, Not DNSSEC, DNSSEC Aware, Validator
  - When not in full compliance add "Partial" in front and "[explanation]" behind
    - Partial Validator[DNAME]
    - Partial DNSSEC Aware[NoBig]

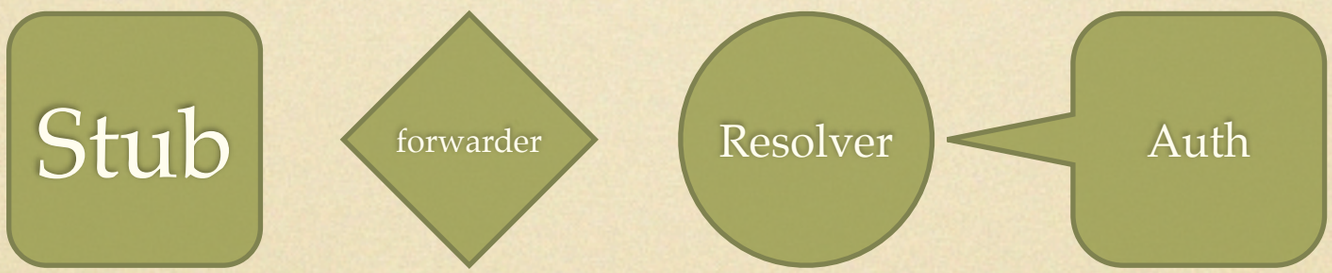
TOOL: DNSSEC RESOLVER

- Java code, Python soon
  - on GitHub
    - https://github.com/ogud/DNSSEC-resolver-check
- Command line app and applet try
  - http://superawesum.novas.us/DSC-3/DSC-3.php

What is a resolver?

- Resolver is an address
  - Standard model:

  - Common edge case:



- Not so fast !!!

How many resolvers per address?

- Anycast DNS resolvers => resolver cluster
  - two subsequent queries go to different instances
- Resolver clusters are flat or include forwarding,
  - “responding” node on edge
  - “lookup” nodes perform recursion

DNS proxies

- For all practical purposes proxies are forwarders
- BUT
  - Proxies hide actual resolvers ==> proxies can give actual open resolvers bad name
    - Hotel net advertises 8.8.8.8 but does not always send query to 8.8.8.8

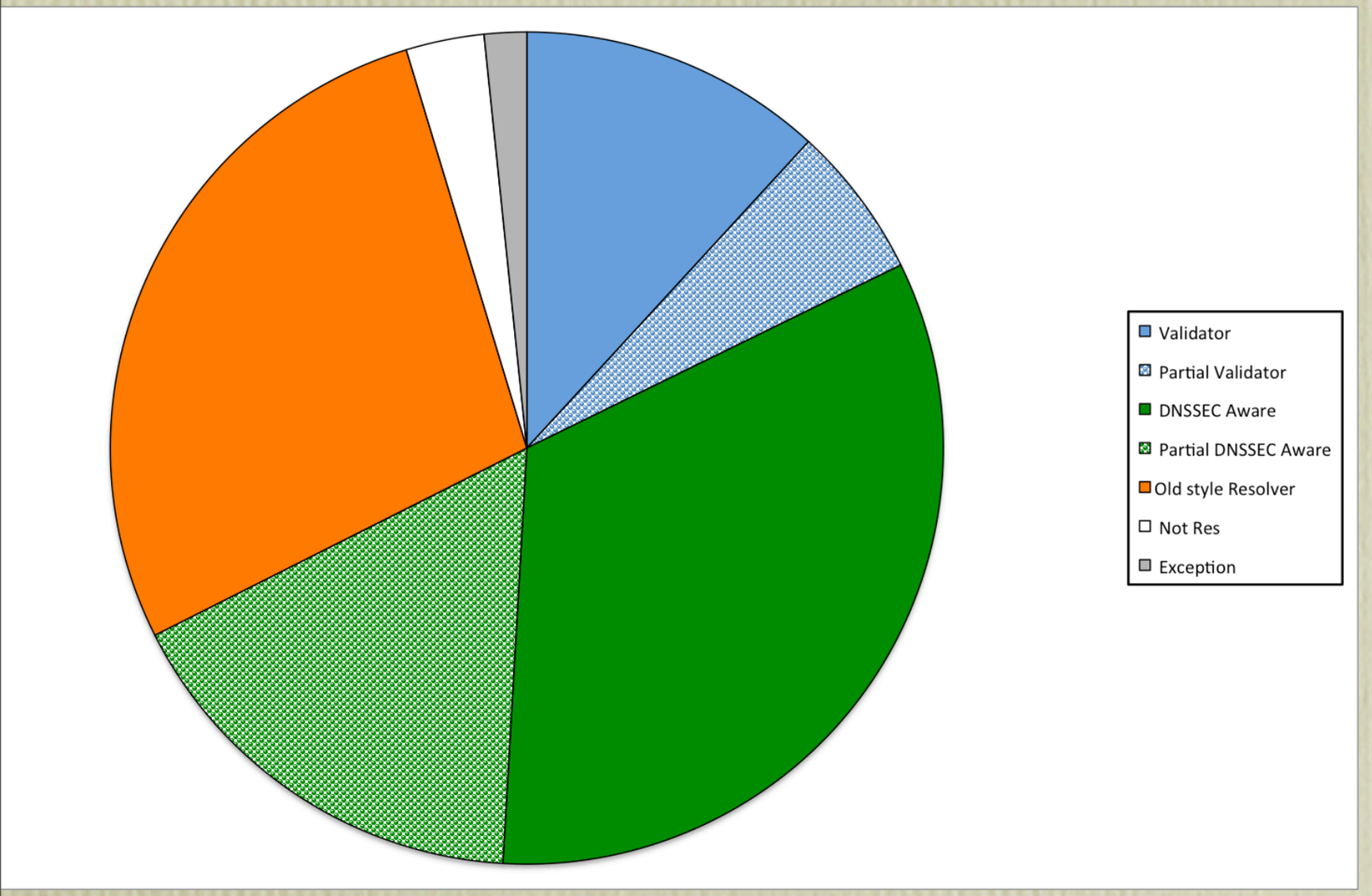
Moral:

- DRC (DNSSEC-Resolver-Check) is not accurate when
  - resolver cluster nodes differ in capability
  - forwarders use resolvers with different capability
  - DNS timeouts occur
  - the edge link degrades resolver if path/middle-box is bad
- Hard to actually classify a particular “resolver”

Resolver Studies:

- Two samples:
  - Sample of US ISP's from Sam Knows
  - Scanned the whole internet and looked for resolvers

Sam Knows Data:



>1/6 Validators
- 2/3 Full Validators
- 1/3 Partial

1/2 DNSSEC Aware
- 2/3 Full
- 1/3 Partial

>1/4 Broken

~ 5% Other

Sample of Residential US resolvers

Scanning whole IPv4 space

Test site sent a basic DNS query to each IPv4 address

- The query was tailored to the address being “Probed”
  - 001-022-123-021.res.dnssecready.net. A
  - This query was resolvable only via a special Shinkuro name server.
  - We record the address probed, the external address of resolver (Query address), and the address query is returned from (Response Address).

Thus, we can track the queries we sent, and we could see the resolver trying to fetch the answer from our name server.

This gave us insight into which resolvers were forwarding to other resolvers versus sending queries to our name servers

By resolving via signed zone we were able to measure resolvers that validated.

Resolver Scan

IPv4 space	4,294,967,295
Addresses probed	3,421,239,040
Dropped responses	10,197,657
Full responses	26,603,239
• “Good” responses	11,697,272
• Well-formed responses	5,908,002

Probably overran our nameserver bandwidth

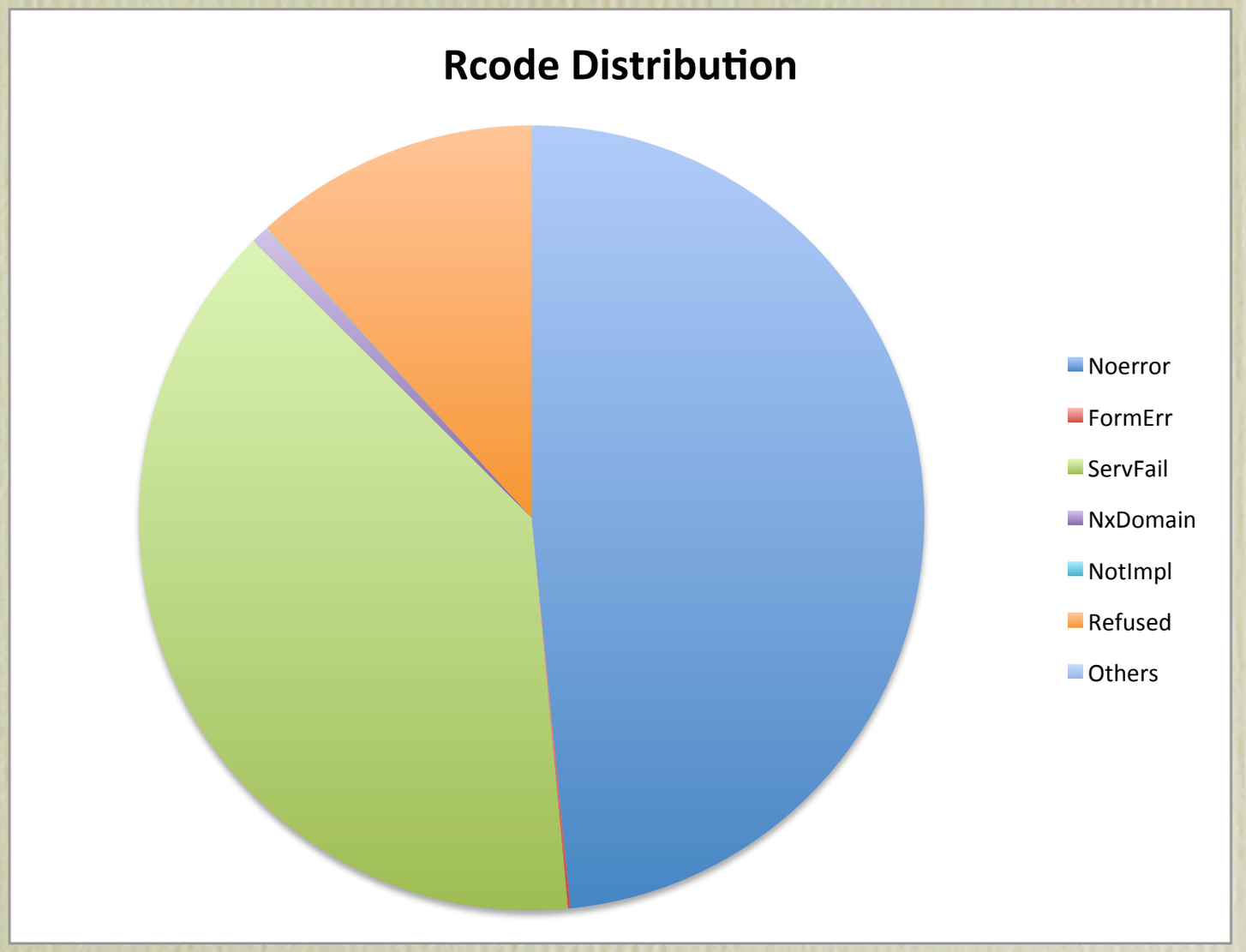
Most of these were evaluated as Not a Resolver or alternately, we had timeout issues.

This part of the testing needs to be redone.

What we found

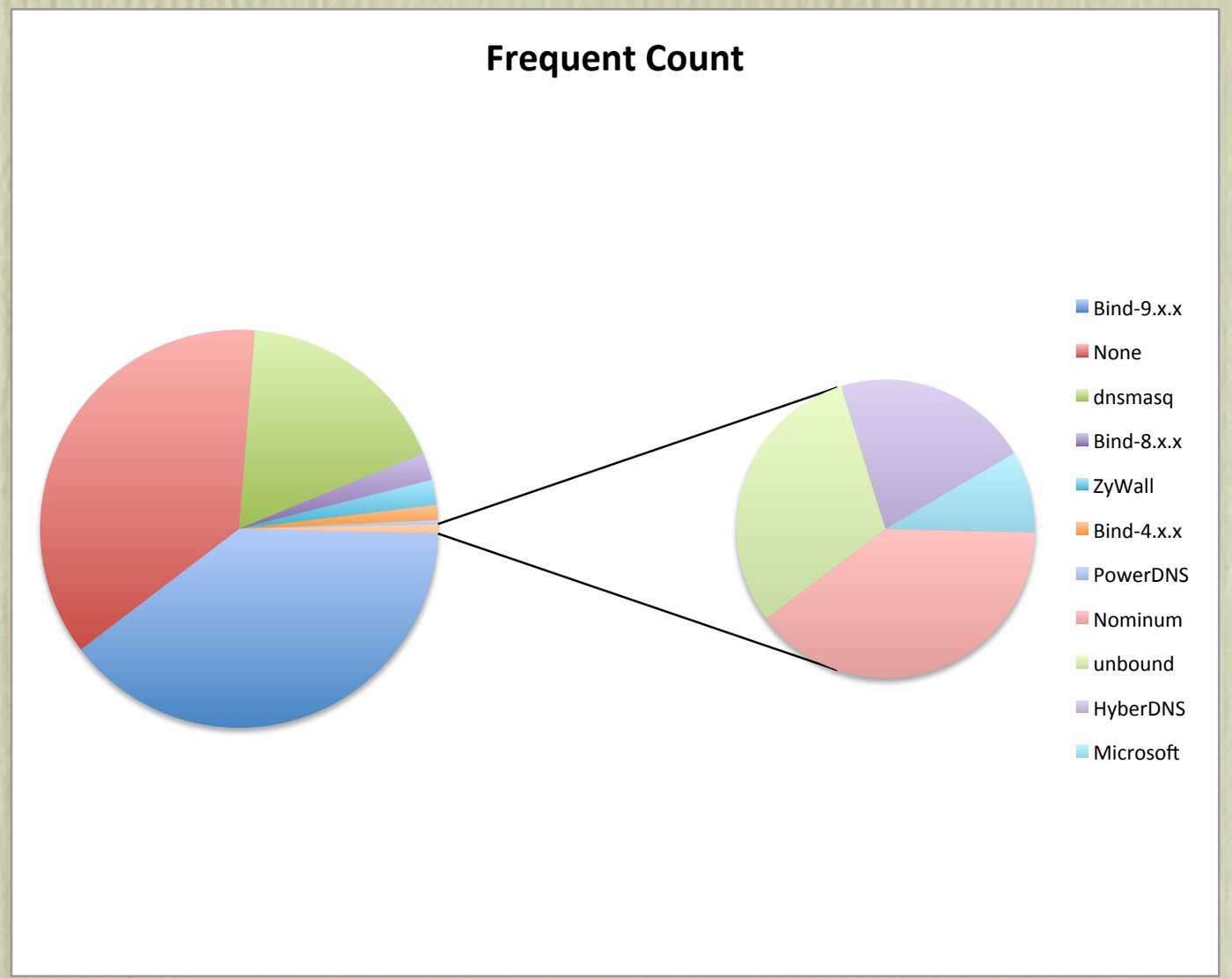
- Answers come back from different ports/addresses
- Lots of Refused and Root Referrals
  - 12,342K vs 11,697K “answers”
  - i.e. over 30M DNS responders on net
- Almost no complaints about the scan
- Some /16 have over 30K responders i.e. ISP supplies open forwarder to customers.
- We can use open forwarders to map that Networks DNS infrastructure
- Asking version.bind. txt ch sometimes allows us to map it to upstream resolver software.

Rcode Distribution



ServFail == Lookup errors
i.e. our server link problem

What is forwarding queries?



Sample of 300,000 sensical responses to: version.bind.

Forwarders vs Resolvers

- Resolver == address query to auth server arrives from

Seen #	Count	Behind it
1	277,433	277,433
2 ..10	79,060	272,759
11 .. 100	23,262	822,300
101 .. 1,000	10,881	3,395,729
1,001 .. 10K	4,532	14,445,698
10K .. 100K	907	24,174,523
100K ..	34	4,916,315

550K out of 40+M

Forwarders

Conclusions

- Hard to classify a resolver unless you are talking directly to an unicast address
- Resolvers are better than we expected
- Forwarders are MUCH more common than we thought
- Thanks to:
  - Ray Bellis for Evldns,
  - Brian Wellington and Bob Halley for Dnsjava and DnsPython
  - Warren Kumari for server, network bandwidth and sacrificial address.