Quantifying DNSSEC Validators

Yingi Yu & Duane Wessels

October, 2012

VERISIGN

Motivation

- How is client-side DNSSEC deployment progressing?
- Informs discussions about issues such as rolling root zone keys.
- Do validators have fingerprints?
- What percent of com/net responses are validated?

Related Work

- "Observing DNSSEC Validation in the Wild"
  - Guðmundsson and Crocker, SATIN 2011
  - Analyzed queries to .ORG name servers.
- "Measuring Occurrence of DNSSEC Validation"
  - Wander and Weis
  - browser-based (1x1 images and javascript)
- "Counting DNSSEC"
  - Geoff Huston/RIPE
  - browser-based (advertisement images)

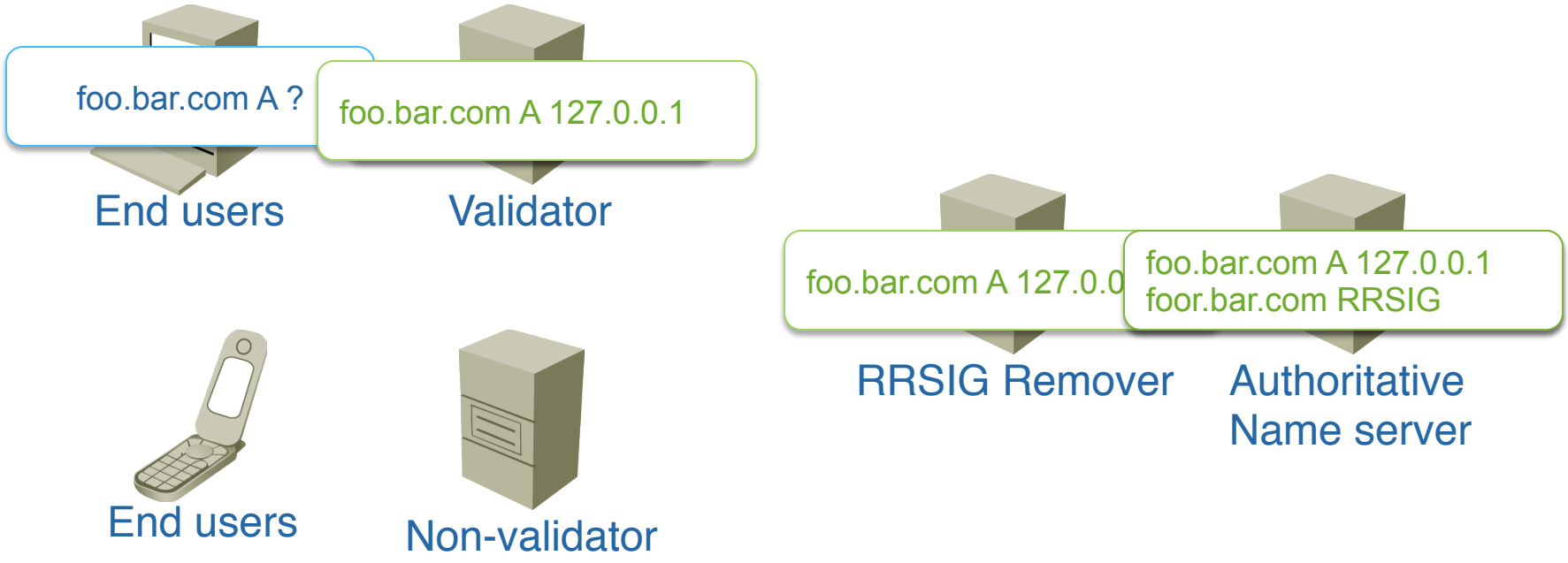
VERISIGN

Our Approach

- DNS-based
  - some help from browser DNS prefetching
- Relies on validators to retry if given a mal-signed response.
- An RRSIG-remover sits in front of signed zones.
  - First response, RRSIG is removed (A query only)
  - Subsequent responses have all signatures
- Initial queries are redirected to unique query names with CNAME response.

How to find a validator?

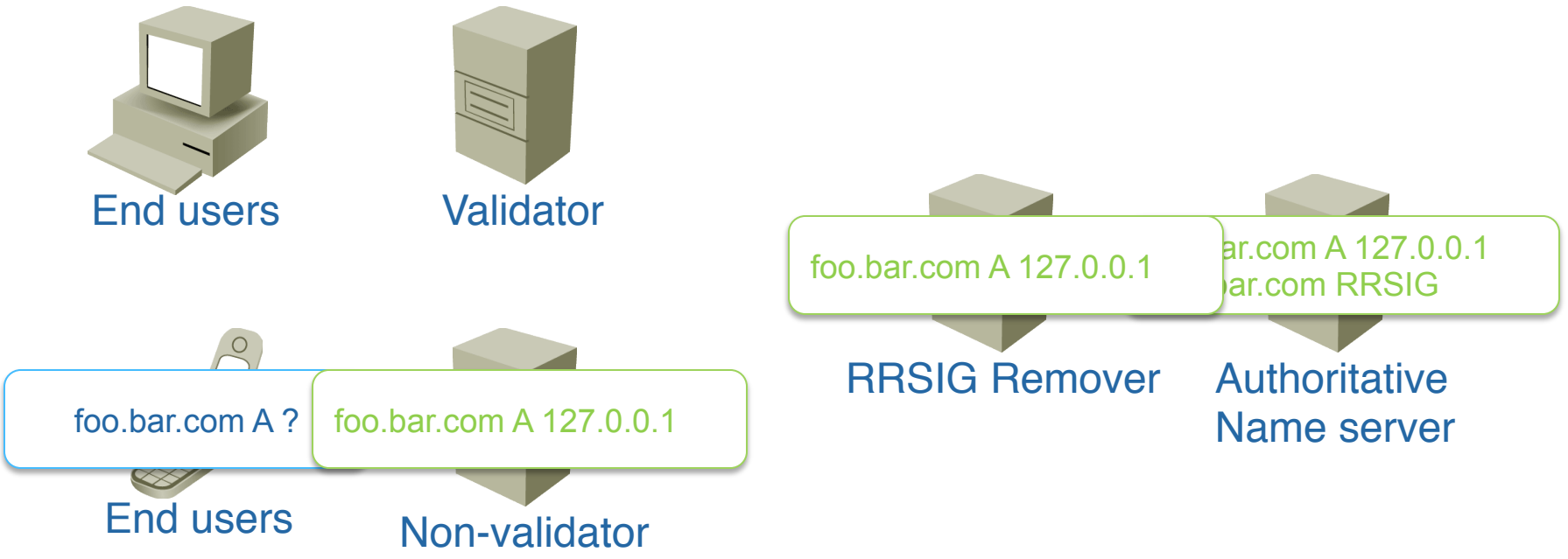
Evidence of DNSSEC Validators



VERISIGN

How to find a validator?

Evidence of Non-Validators



VERISIGN

Complications with Our Method

- Needs retry behavior, which is inconsistent and not required by RFCs.
  - But seems to work reasonably well for this experiment.
- Packet loss could be interpreted as validation.
  - Reduced by examining multiple lookups over course of a day.
  - Other causes of repeated queries?
- Fails to find a validator behind a forwarder.
  - Retries don’t make it past the forwarder.

VERISIGN

WPAD

- The Web Proxy Auto Discovery protocol says that HTTP agents should query for wpad.$domainname in order to locate a proxy autoconfiguration file.
- Naturally, some implementations will query for wpad.$tld, or even “wpad.”
- Duane registered wpad.{com,net,org,biz,us} shortly after reading the internet-draft. Hooray!
- These domains receive ~2,000,000 queries per day.

VERISIGN

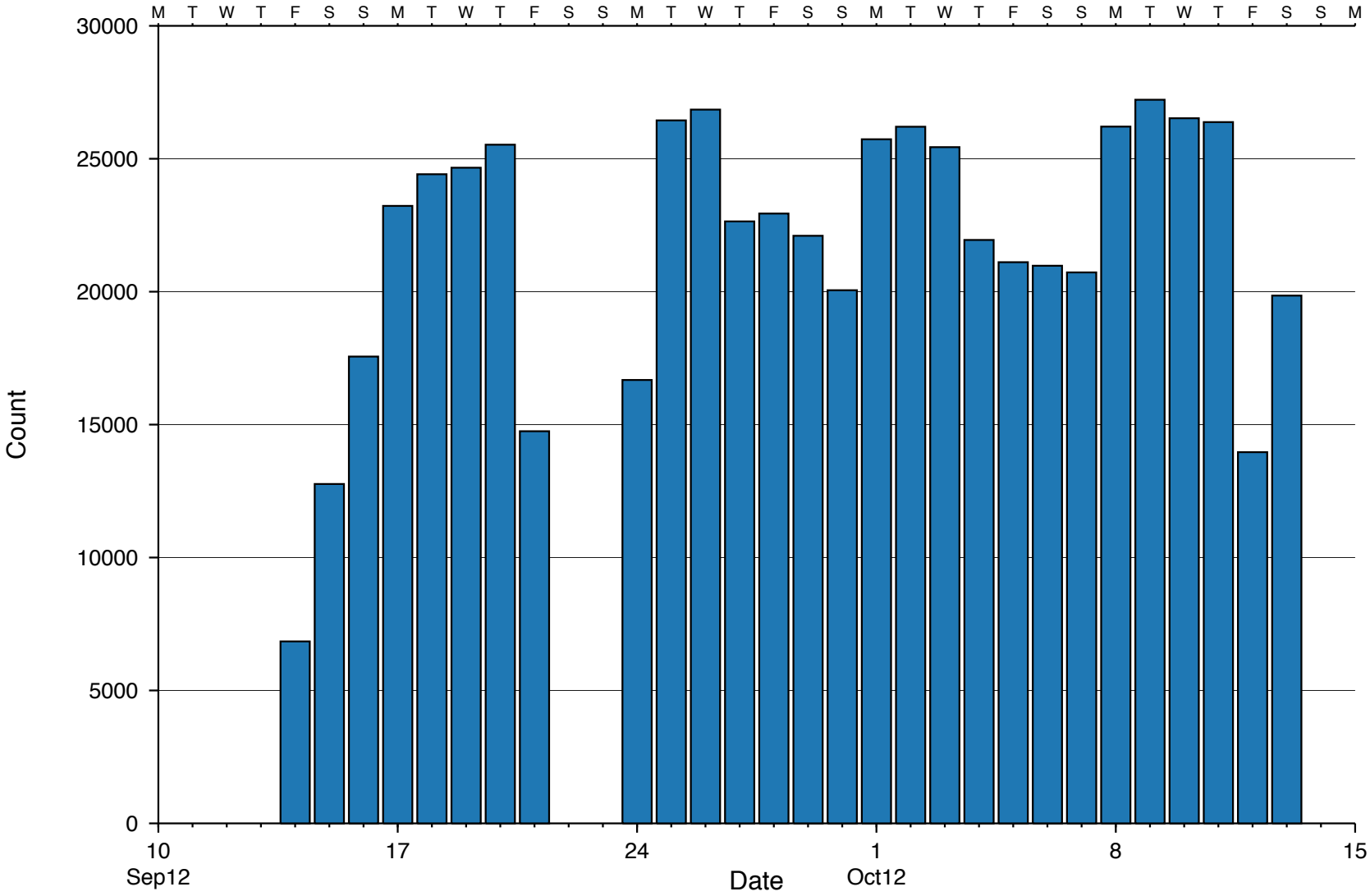
Prefetching

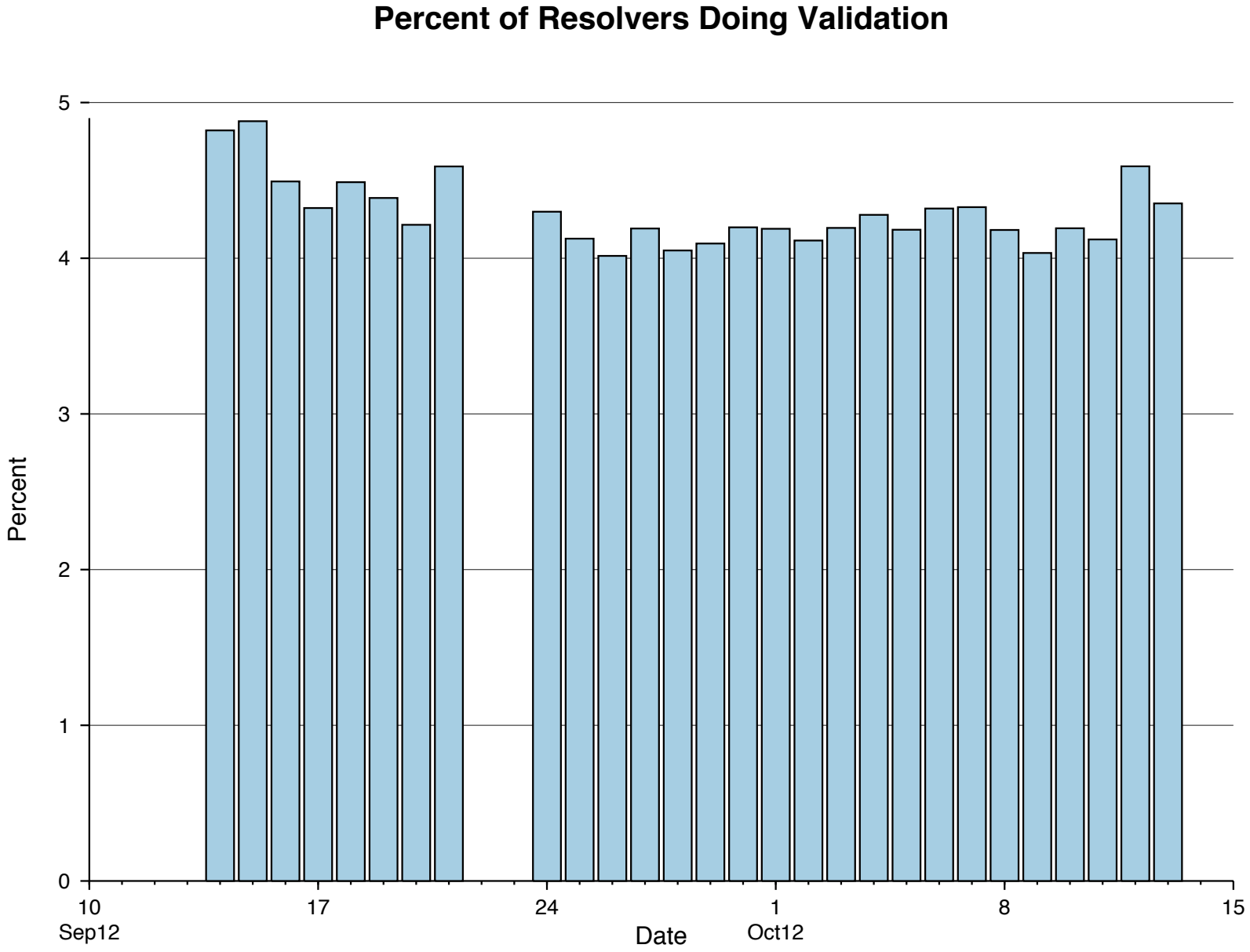
- We asked people to add the following line to web pages in order to drive DNS queries to us:

- Most browsers will automatically pre-fetch the DNS name.

Results

Number of Resolvers Observed




Percent of Resolvers Doing Validation
Percent
5
4
3
2
1
0
10
Sep12
17
24
1
Oct12
8
15
Date

Comparison with All Resolvers Seen at COM/NET sites

- October 11, 2012
- 4 Verisign sites: AMS, IAD, NYC, SFO

- 4,801,160 unique IPs seen at sites
- 26,379 (5.5%) unique resolver IPs observed by test
- 1,087 (0.023%) unique validator IPs found by test

- 19,197,063,214 total queries received at sites
- 9,296,623,161 (48.4%) queries from observed resolvers
- 1,449,625,183 (7.6%) queries from observed validators

VERISIGN

Geographic Distribution

CC	#Resolvers	%Validators	CC	#Resolvers	%Validators	CC	#Resolvers	%Validators
SE	145	46.2%	UA	161	4.3%	AR	446	1.8%
CZ	197	33.5%	PL	474	4.0%	RU	701	1.6%
BR	1098	13.6%	GB	569	3.7%	HK	130	1.5%
NL	267	10.1%	JP	519	3.3%	PH	205	1.5%
DE	577	8.8%	TH	124	3.2%	TW	950	1.3%
CH	182	7.7%	AU	224	3.1%	IT	278	1.1%
ID	173	7.5%	BE	133	3.0%	RO	214	0.9%
TR	110	5.5%	US	10306	2.8%	IN	468	0.9%
CL	315	5.1%	CA	654	2.6%	ES	249	0.8%
AT	121	5.0%	CN	1302	2.5%	MX	250	0.8%
FR	1093	4.7%	BG	109	1.8%	KR	545	0.0%
CO	113	4.4%	HU	110	1.8%	??	109	0.0%

For Countries with 100 or more resolvers observed

VERISIGN

Fingerprints

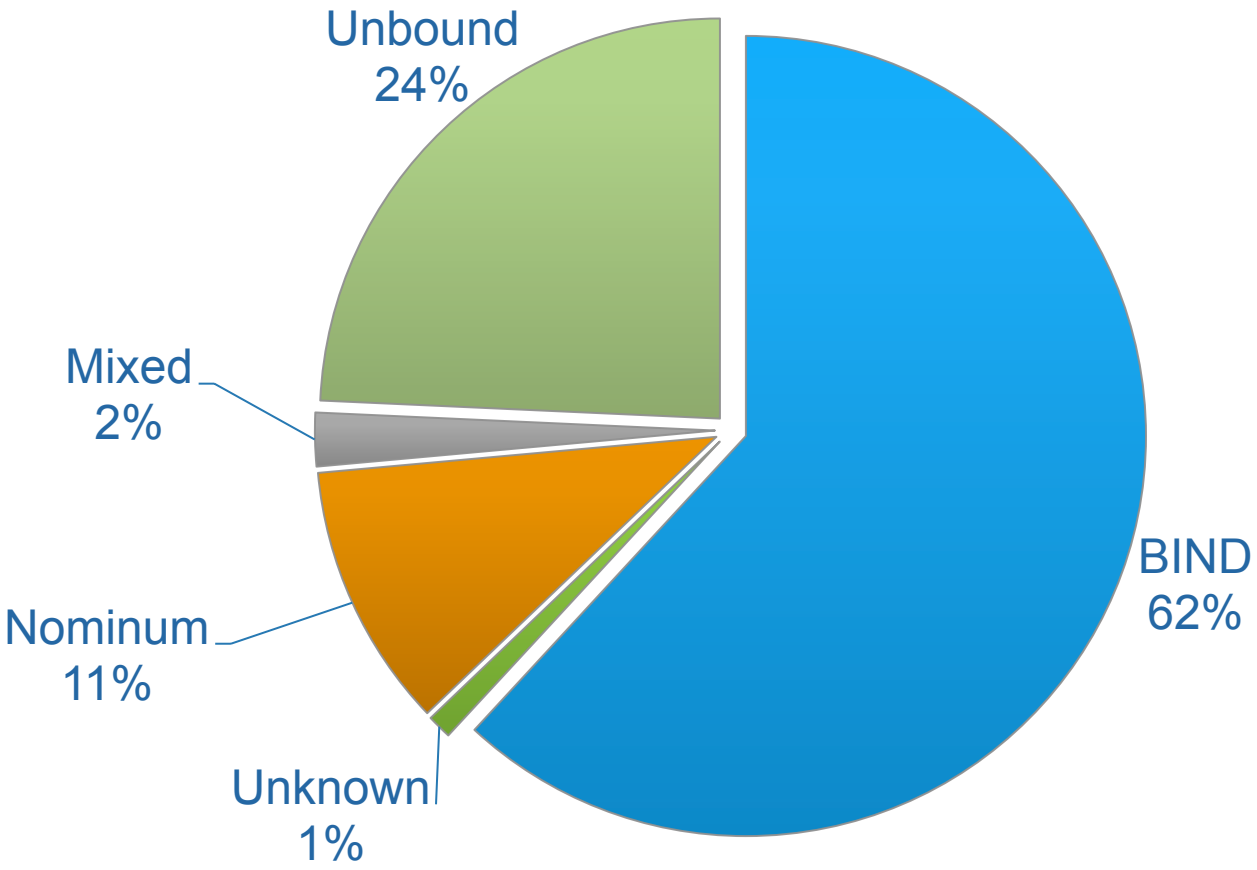
- The order of queries allows us to identify the name server software.

BIND 9.[78] | Unbound 1.4 | Nominum* | Unknown

- Nominum DNS does not requery for other types of RRs if signature is missing.

VERISIGN

Fingerprints



Comparison With Related Work

Comparison

- Guðmundsson and Crocker
  - “In both periods the percentage of confirmed validators is about 1.2 percent of the total number of resolvers…”
  - November 2010, January 2011
- Wander and Weis
  - “Overall 3,443 trials were positive (4.5%) …”
  - Note, these are “trials,” not resolvers
- Huston
  - “2,316 out of 57,267, or **4.0%** of the DNS resolvers were observed to perform DNSSEC validation”

Project Website

http://validator-search.verisignlabs.com/

Thank You

VERISIGN