Measuring DNSSEC Use

Geoff Huston
APNIC Labs

We all know…

We all know…

what DNSSEC does.

We all know…

And why its probably a Good Thing to do if you are a zone admin or a DNS resolver operator

We all know…

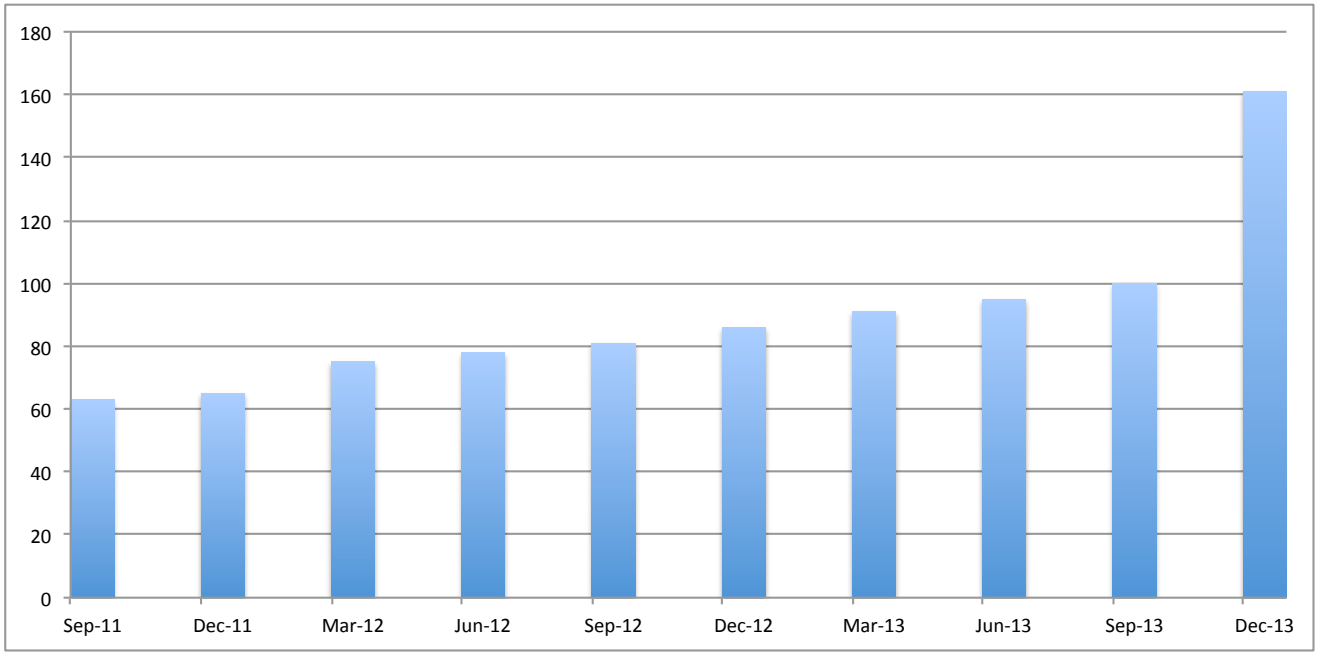
And why its probably a Good Thing to do if you are a zone admin or a DNS resolver operator.

And why its probably good for end users to use DNSSEC-validating resolvers as well.

We all know…

And we've all seen various measurements of how many zones are DNSSEC-signed…

DNSSEC-Signed TLDs at the Root



We all know…

And we've all seen various m… how many zones are DNSSE…

But these are generally supply-side measurements

What about the demand size?

if you sign it will they come to validate it?

But what we don't know is…

What will happen to your authoritative name server when you serve a signed zone?

Will you experience:

- Query load meltdown?
- TCP session overload?
- DDOS amplification from hell?
- No change?

Our Questions…

- What proportion of the Internet's users will perform DNSSEC validation if they are presented with a signed domain?
- Where are these DNSSEC-validating users?
- What is the performance overhead of serving signed names?
- What happens when the DNSSEC signature is not valid?

The Experiment

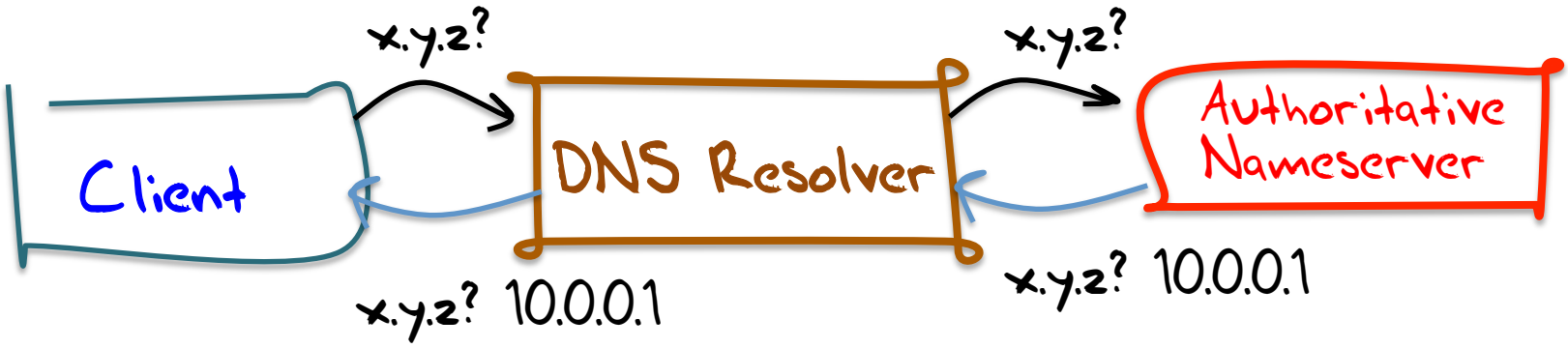
Three URLs:

- the good (DNSSEC signed)
- the bad (invalid DNSSEC signature)
- the control (no DNSSEC at all)

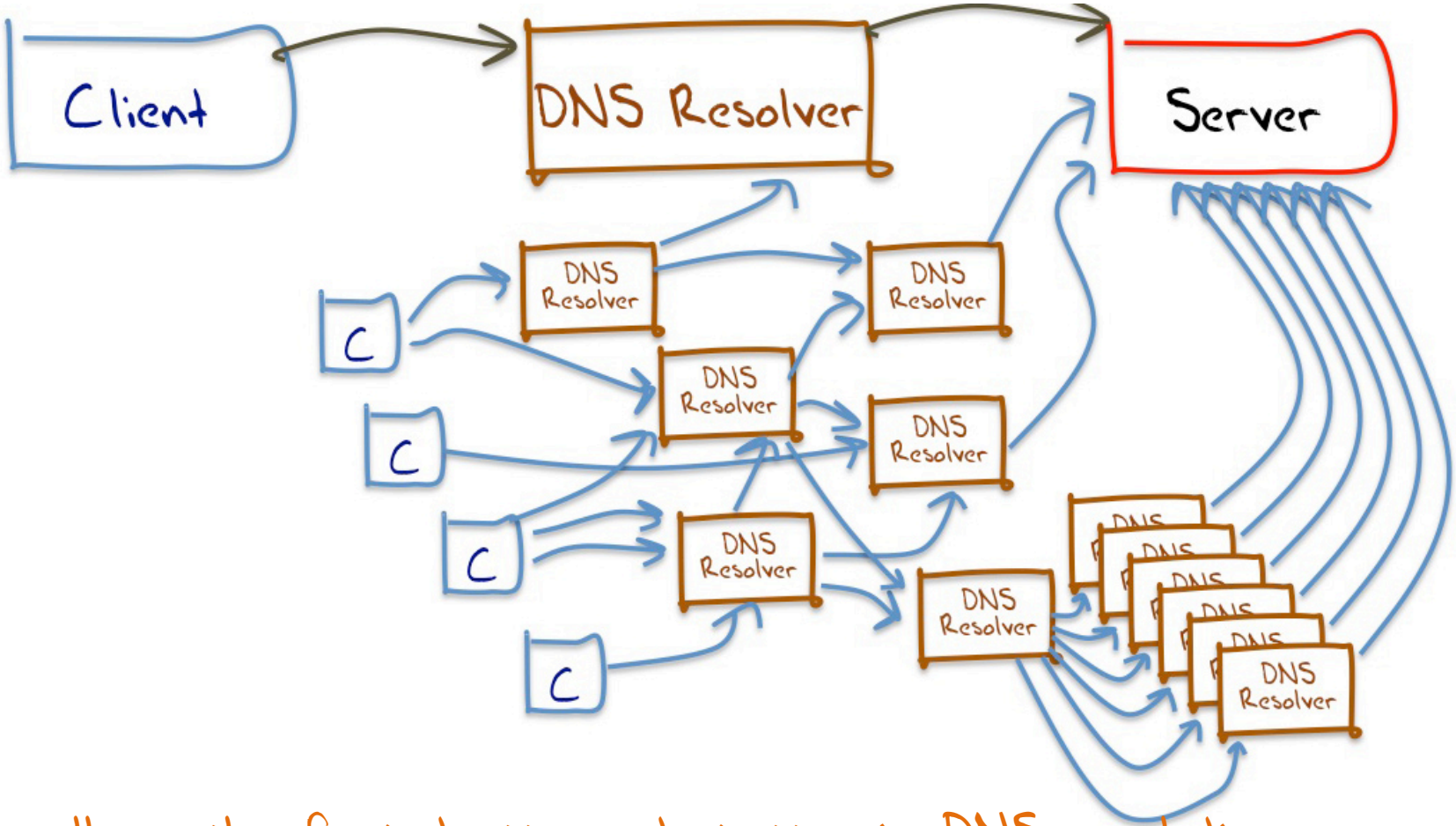
And an online ad system to deliver the test to a large pseudo-random set of clients

Understanding DNS Resolvers is "tricky"

What we would like to think happens in DNS resolution!

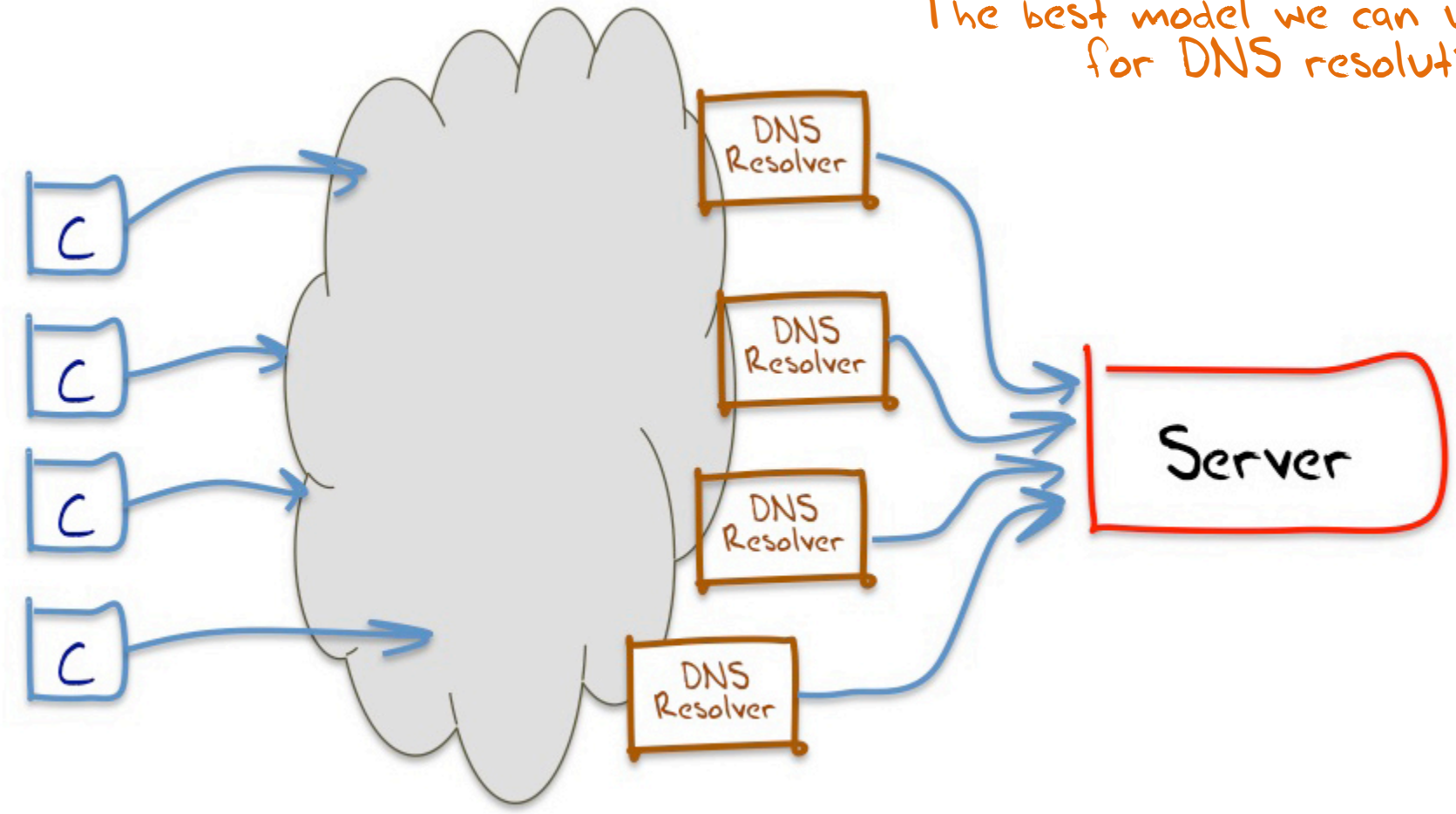


Understanding DNS Resolvers is "tricky"

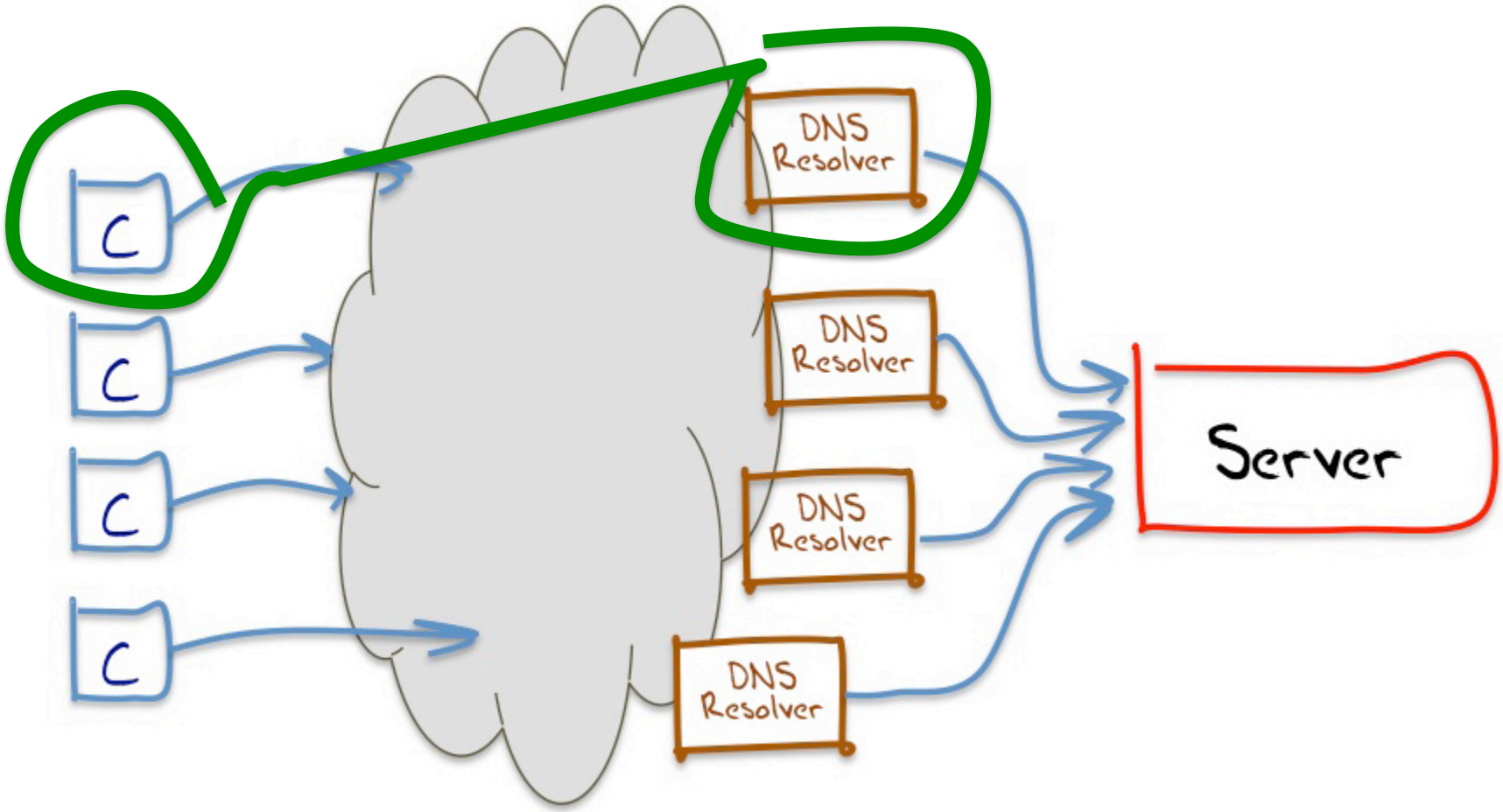


A small sample of what appears to happen in DNS resolution

Understanding DNS Resolvers is "tricky"



Understanding Resolvers is "tricky"



if we combine www and dns data we can map clients to the visible resolvers that query our server

This means…

That it's hard to talk about "all resolvers"

- We don't know the ratio of the number of resolvers we cannot see compared to the resolvers we can see from the perspective of an authoritative name server

We can only talk about "visible resolvers"

This means…

And there is an added issue here:

- It can be hard to tell the difference between a visible resolver performing DNSSEC validation and an occluded validating resolver performing validation via a visible non-validating forwarder

(Yes, I know it's a subtle distinction, but it makes looking at RESOLVERS difficult!)

This means…

It's easier to talk about end clients rather than resolvers, and whether these end clients use / don't use a DNS resolution service that performs DNSSEC validation

On to Some Results

December 2013

- Presented: 5,683,295 experiments to clients
- Reported: 4,978,829 experiments that ran to "completion"

Web results for clients:

- Did Not Fetch invalidly signed object: **7.1%**
- Fetched all URLs: **92.9%**

That means…

That 7.1% of clients use DNSSEC validating resolvers, because these clients did not fetch the object that had the invalid DNSSEC signature

Right?

That means…

That 7.1% of clients use DNSSEC validating resolvers, because these clients did not fetch the object that had the invalid DNSSEC signature

Right?

Well, not really, due to the experimental technique.

We can learn more if we look at the logs of the DNS queries…

Refining these Results

December 2013

- Presented: 5,683,295 experiments
- Reported: 4,978,929 experiments that ran to "completion"

Web + DNS query log results for clients:

- Performed DNSSEC signature validation and did not fetch the invalidly signed object: **6.8%**
- Fetched DNSSEC RRs, but then retrieved the invalidly signed object anyway: **4.7%**
- Did not have a DNSSEC clue at all - only fetched A RRs: **88.5%**

That means…

That **6.8%** of clients appear to be performing DNSSEC validation and not resolving DNS names when the DNSSEC signature cannot be validated

A further **4.7%** of clients are using a mix of validating and non-validating resolvers, and in the case of a validation failure turn to a non-validating resolver!

Where is DNSSEC? - The Top 20

Rank	CC Code	Tests	Validating (%)	Mixed (%)	None (%)	
1	YE	2,279	70.8%	11.2%	18.0%	Yemen
2	SE	5,983	67.2%	4.6%	28.2%	Sweden
3	SI	5,883	51.0%	6.1%	42.9%	Slovenia
			44.7%	4%	50.9%	onia
		4,996	42.4%	3%	45.8%	m
		3,556	41.0%	4%	55.	
		10,468	30.8%	4%	60.	
		1,204	29.8%	6%	58.	
		110,380	26.8%	6%	64.	
10	CL				70.	
11	ZA				68.	
12	UA				65.2%	Ukraine
13	ID				68.2%	Indonesia
14	IE				76.3%	Ireland
15	TZ				63.8%	Tanzania
16	CO				73.3%	Colombia
17	DZ				43.4%	Algeria
18	PS				53.2%	Occupied Palestinian T.
19	AZ	5,095	18.2%	18.4%	63.4%	Azerbaijan
20	US	311,740	15.2%	3.5%	81.3%	United States of America
	XA	**5,331,072**	**6.7%**	**4.8%**	**88.5%**	**World**

% of clients who appear to use only DNSSEC-validating resolvers

% of clients who use a mix of DNSSEC-validating resolvers and non-validating resolvers

% of clients who use non-validating resolvers

Geo-locate clients to countries, and select countries with more than 1,000 data points

Where is DNSSEC? - The Top 20

Rank	CC Code	Tests	Validating (%)	Mixed (%)	None (%)	
1	YE	2,279	70.8%	11.2%	18.0%	Yemen
2	SE	5,983	67.2%	4.6%	28.2%	Sweden
3	SI	5,883	51.0%	6.1%	42.9%	Slovenia
4	EE	2,132	44.7%	4.4%	50.9%	Estonia
5	VN	114,996	42.4%	11.8%	45.8%	Vietnam
6	FI	3,556	41.0%	3.4%	55.6%	Finland
7	CZ	10,468	30.8%	8.4%	60.9%	Czech Republic
8	LU	1,204	29.8%	11.6%	58.6%	Luxembourg
9	TH	110,380	26.8%	8.6%	64.7%	Thailand
10	CL	21,167	26.6%	2.8%	70.7%	Chile
11	ZA	12,398	26.2%	5.8%	68.0%	South Africa
12	UA	32,916	25.0%	9.8%	65.2%	Ukraine
13	ID	89,331	22.0%	9.8%	68.2%	Indonesia
14	IE	7,679	20.7%	3.0%	76.3%	Ireland
15	TZ	1,724	20.7%	15.6%	63.8%	Tanzania
16	CO	25,440	20.3%	6.5%	73.3%	Colombia
17	DZ	16,198	19.1%	37.5%	43.4%	Algeria
18	PS	8,441	18.5%	28.3%	53.2%	Occupied Palestinian T.
19	AZ	5,095	18.2%	18.4%	63.4%	Azerbaijan
20	US	311,740	15.2%	3.5%	81.3%	United States of America
	XA	**5,331,072**	**6.7%**	**4.8%**	**88.5%**	**World**

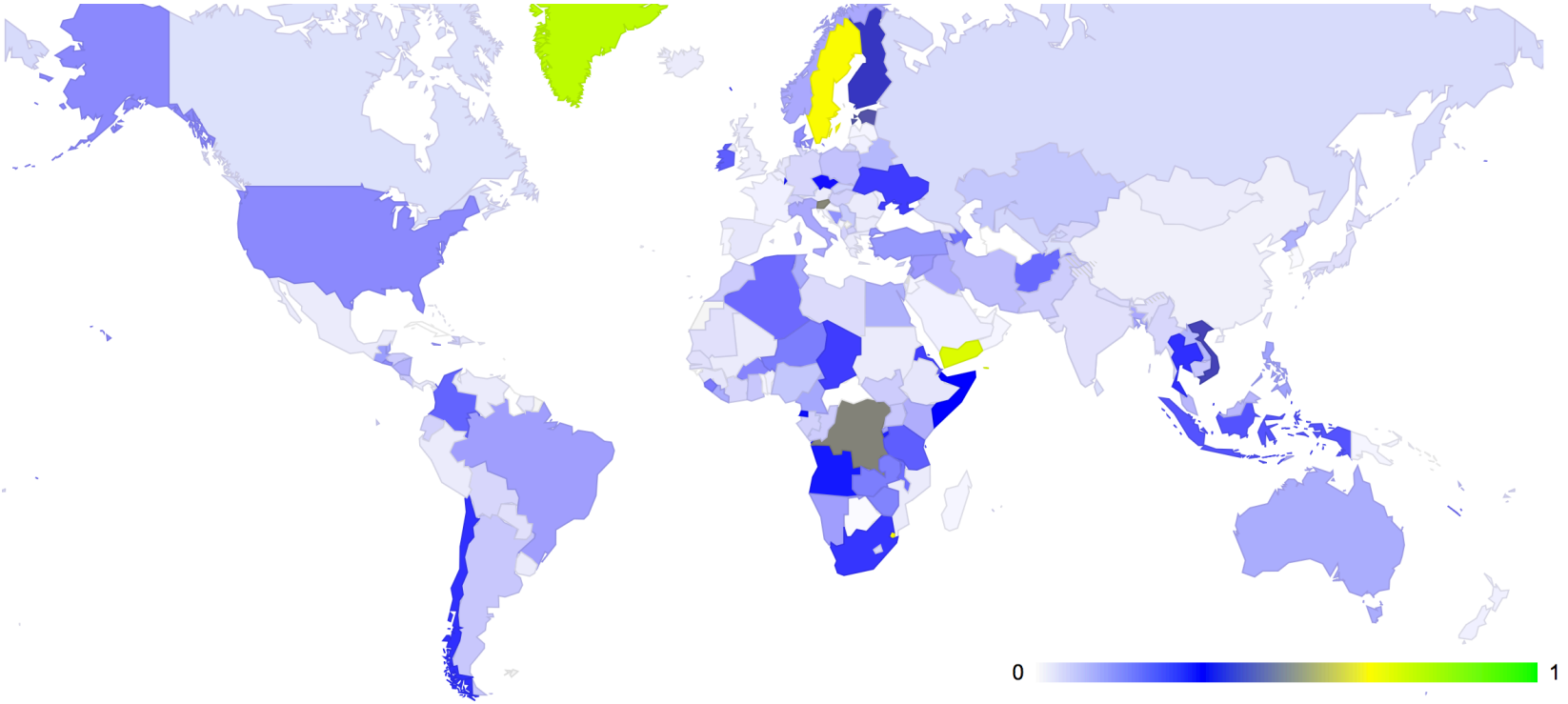
Geo-locate clients to countries, and select countries with more than 1,000 data points

Where is DNSSEC? - The bottom 20

Rank	CC Code	Tests	Validating (%)	Mixed (%)	None (%)	
97	CN	1,215,241	1.9%	2.1%	96.0%	China
98	SA	45,243	1.7%	2.1%	96.2%	Saudi Arabia
99	MD	3,168	1.6%	1.9%	96.5%	Republic of Moldova
100	FR	86,888	1.6%	1.0%	97.4%	France
101	NZ	31,683	1.6%	15.0%	83.4%	New Zealand
102	BE	15,243	1.5%	3.8%	94.7%	Belgium
103	PR	3,521	1.5%	13.0%	85.5%	Puerto Rico
104	LT	14,984	1.4%	1.7%	96.9%	Lithuania
105	SG	36,420	1.4%	4.8%	93.8%	Singapore
106	BS	1,158	1.4%	2.7%	95.9%	Bahamas
107	HR	8,856	1.4%	1.2%	97.5%	Croatia
108	OM	6,147	1.3%	2.0%	96.7%	Oman
109	TT	2,497	1.3%	3.4%	95.3%	Trinidad and Tobago
110	ME	3,552	1.3%	3.5%	95.3%	Montenegro
111	LV	2,041	1.2%	3.3%	95.4%	Latvia
112	PT	17,641	1.2%	2.0%	96.8%	Portugal
113	MU	3,452	1.1%	1.7%	97.2%	Mauritius
114	BH	4,231	1.1%	5.7%	93.2%	Bahrain
115	AE	47,996	1.0%	1.0%	98.0%	United Arab Emirates
116	JO	10,527	0.9%	1.3%	97.9%	Jordan
117	QA	15,975	0.4%	0.8%	98.8%	Qatar
118	KR	668,885	0.3%	0.4%	99.3%	Republic of Korea
	XA	**5,331,072**	**6.7%**	**4.8%**	**88.5%**	**World**

Geo-locate clients to countries, and select countries with more than 1,000 data points

The Mapped view of DNSSEC Use



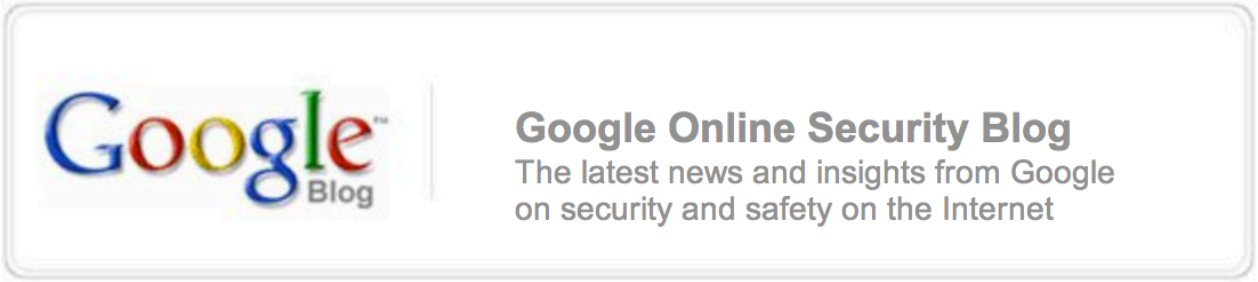
Fraction of users who use
DNSSEC-validating resolvers

Why

is it that 7% of users performing DNSSEC validation is about 3 times the number of users who are capable of using IPv6?

Why has DNSSEC deployment been so successful compared to IPv6?

Is Google's P-DNS a Factor?



Google Public DNS Now Supports DNSSEC Validation

Tuesday, March 19, 2013 8:30 AM
Posted by Yunhong Gu, Team Lead, Google Public DNS

We launched Google Public DNS three years ago to help make the Internet faster and more secure. Today, we are taking a major step towards this security goal: we now fully support DNSSEC (Domain Name System Security Extensions) validation on our Google Public DNS resolvers. Previously, we accepted and forwarded DNSSEC-formatted messages but did not perform validation. With this new security feature, we can better protect people from DNS-based attacks and make DNS more secure overall by identifying and rejecting invalid responses from DNSSEC-protected domains.

DNS translates human-readable domain names into IP addresses so that they are accessible by computers. Despite its critical role in Internet applications, the lack of security protection for DNS up to this point meant that a significantly large portion of today's Internet attacks target the name resolution process, attempting to return the IP addresses of malicious websites to DNS queries. Probably the most common DNS attack is DNS cache poisoning, which tries to "pollute" the cache of DNS resolvers (such as Google Public DNS or those provided by most ISPs) by injecting spoofed responses to upstream DNS queries.

Another observation from the data

Clients who used Google's Public DNS servers: **10.4%**

- Exclusively Used Google's P-DNS: **5.4%**
- Used a mix of Google's P-DNS and other resolvers: **5.0%**

Is Google's P-DNS a Factor?

		DNSSEC Validation		Google Public DNS			
Rank	CC Code	Tests	Validating	All	Mixed	None	
1	YE	2,279	70.8%	6.5%	5.0%	88.5%	Yemen
			7.2%	2.1%	0.4%	97.5%	Sweden
				5.0%	0.4%	94.7%	Slovenia
			%	4.2%	1%	94.8%	nia
			2.4%	98.7%	1.3%	0.1%	
			1.0%	2.1%	0.8%	9	
			0.8%	13.8%	1.5%	7	
			9.8%	15.9	0.8%	8	
			6.8%	15	5.9%	7	
10	CL	21,167	26.6%		0.4%	9	
11	ZA	12,				8	
12	UA	32,				76.9%	Ukraine
13	ID	89,				19.8%	Indonesia
14	IE	7,				81.9%	Ireland
15	TZ	1,				0.6%	Tanzania
16	CO	25,				85.8%	Colombia
17	DZ	16,198	19.1%	71.2%	27.7%	1.1%	Algeria
18	PS	8,441	18.5%	51.8%	29.2%	19.0%	Occupied Palestinian T.
19	AZ	5,095	18.2%	68.5%	9.6%	21.9%	Azerbaijan
20	US	311,740	15.2%	10.6%	2.9%	86.4%	United States of America
	XA	**5,331,072**	**6.7%**	**50.2%**	**7.3%**	**42.5%**	**World**

% of validating clients who exclusively use Google's P-DNS

% of clients who do not use Google's P-DNS service

% of clients who use a mix of Google's P-DNS and other resolvers

Of those clients who perform DNSSEC validation, what resolvers are they using: All Google P-DNS? Some Google P-DNS? No Google P-DNS?

Is Google's P-DNS a Factor?

		DNSSEC Validation		Google Public DNS			
Rank	**CC Code**	**Tests**	**Validating**	**All**	**Mixed**	**None**	
1	YE	2,279	70.8%	6.5%	5.0%	88.5%	Yemen
2	SE	5,983	67.2%	2.1%	0.4%	97.5%	Sweden
3	SI	5,883	51.0%	5.0%	0.4%	94.7%	Slovenia
4	EE	2,132	44.7%	4.2%	1.1%	94.8%	Estonia
5	VN	114,996	42.4%	98.7%	1.3%	0.1%	Vietnam
6	FI	3,556	41.0%	2.1%	0.8%	97.1%	Finland
7	CZ	10,468	30.8%	13.8%	6.5%	79.7%	Czech Republic
8	LU	1,204	29.8%	15.9%	0.8%	83.3%	Luxembourg
9	TH	110,380	26.8%	15.9%	5.9%	78.3%	Thailand
10	CL	21,167	26.6%	6.2%	0.4%	93.4%	Chile
11	ZA	12,398	26.2%	8.0%	3.0%	89.0%	South Africa
12	UA	32,916	25.0%	20.1%	3.0%	76.9%	Ukraine
13	ID	89,331	22.0%	72.2%	8.1%	19.8%	Indonesia
14	IE	7,679	20.7%	17.0%	1.1%	81.9%	Ireland
15	TZ	1,724	20.7%	94.4%	5.1%	0.6%	Tanzania
16	CO	25,440	20.3%	12.7%	1.5%	85.8%	Colombia
17	DZ	16,198	19.1%	71.2%	27.7%	1.1%	Algeria
18	PS	8,441	18.5%	51.8%	29.2%	19.0%	Occupied Palestinian T.
19	AZ	5,095	18.2%	68.5%	9.6%	21.9%	Azerbaijan
20	US	311,740	15.2%	10.6%	2.9%	86.4%	United States of America
	XA	**5,331,072**	**6.7%**	**50.2%**	**7.3%**	**42.5%**	**World**

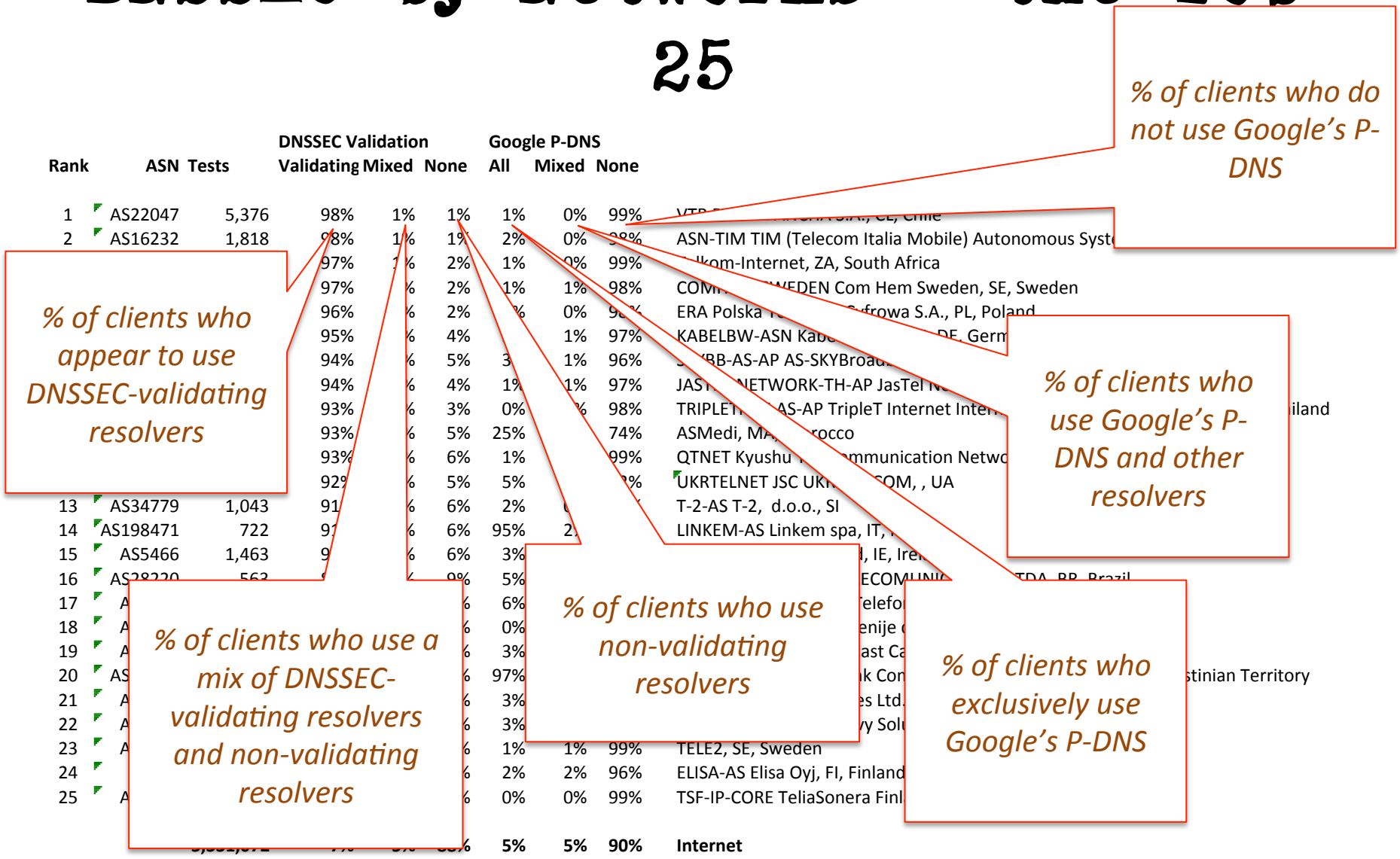
Of those clients who perform DNSSEC validation, what resolvers are they using: All Google P-DNS? Some Google P-DNS? No Google P-DNS?

Is Google's P-DNS a Factor?

		DNSSEC Validation		Google Public DNS			
Rank	CC Code	Tests	Validating	All	Mixed	None	
1	YE	2,279	70.8%	6.5%	5.0%	88.5%	Yemen
2	SE	5,983	67.2%	2.1%	0.4%	97.5%	Sweden
3	SI	5,883	51.0%	5.0%	0.4%	94.7%	Slovenia
4	EE	2,132	44.7%	4.2%	1.1%	94.8%	Estonia
5	VN	114,996	42.4%	98.7%	1.3%	0.1%	Vietnam
6	FI	3,556	41.0%	2.1%	0.8%	97.1%	Finland
7	CZ	10,468	30.8%	13.8%	6.5%	79.7%	Czech Republic
8	LU	1,204	29.8%	15.9%	0.8%	83.3%	Luxembourg
9	TH	110,380	26.8%	15.9%	5.9%	78.3%	Thailand
10	CL	21,167	26.6%	6.2%	0.4%	93.4%	Chile
11	ZA	12,398	26.2%	8.0%	3.0%	89.0%	South Africa
12	UA	32,916	25.0%	20.1%	3.0%	76.9%	Ukraine
13	ID	89,331	22.0%	72.2%	8.1%	19.8%	Indonesia
14	IE	7,679	20.7%	17.0%	1.1%	81.9%	Ireland
15	TZ	1,724	20.7%	94.4%	5.1%	0.6%	Tanzania
16	CO	25,440	20.3%	12.7%	1.5%	85.8%	Colombia
17	DZ	16,198	19.1%	71.2%	27.7%	1.1%	Algeria
18	PS	8,441	18.5%	51.8%	29.2%	19.0%	Occupied Palestinian T.
19	AZ	5,095	18.2%	68.5%	9.6%	21.9%	Azerbaijan
20	US	311,740	15.2%	10.6%	2.9%	86.4%	United States of America
	XA	**5,331,072**	**6.7%**	**50.2%**	**7.3%**	**42.5%**	**World**

Of those clients who perform DNSSEC validation, what resolvers are they using: All Google P-DNS? Some Google P-DNS? No Google P-DNS?

DNSSEC by Networks - the Top 25



Rank	ASN	Tests	DNSSEC Validation: Validating	Mixed	None	Google P-DNS: All	Mixed	None	
1	AS22047	5,376	98%	1%	1%	1%	0%	99%	VTR [illegible]
2	AS16232	1,818	98%	1%	1%	2%	0%	98%	ASN-TIM TIM (Telecom Italia Mobile) Autonomous Syste
			97%	1%	2%	1%	0%	99%	[illegible]kom-Internet, ZA, South Africa
			97%	1%	2%	1%	1%	98%	COM[illegible]WEDEN Com Hem Sweden, SE, Sweden
			96%	1%	2%	1%	0%	99%	ERA Polska [illegible]ufrowa S.A., PL, Poland
			95%	1%	4%	1%	1%	97%	KABELBW-ASN Kabe[illegible]DE, Germ
			94%	1%	5%	3%	1%	96%	[illegible]BB-AS-AP AS-SKYBroad[illegible]
			94%	1%	4%	1%	1%	97%	JAST[illegible]NETWORK-TH-AP JasTel N[illegible]
			93%	1%	3%	0%	2%	98%	TRIPLET[illegible]AS-AP TripleT Internet Inter[illegible]
			93%	1%	5%	25%		74%	ASMedi, MA[illegible]rocco
			93%	1%	6%	1%		99%	QTNET Kyushu [illegible]mmunication Netwo
			92%	1%	5%	5%		93%	UKRTELNET JSC UKR[illegible]COM, , UA
13	AS34779	1,043	91%	1%	6%	2%	0%	98%	T-2-AS T-2, d.o.o., SI
14	AS198471	722	91%	1%	6%	95%	2%	3%	LINKEM-AS Linkem spa, IT, [illegible]
15	AS5466	1,463	9[illegible]	1%	6%	3%	0%	97%	[illegible], IE, Ire[illegible]
16	AS28220	563	[illegible]	1%	9%	5%	0%	95%	[illegible]ECOMUNIC[illegible]TDA, BR, Brazil
17	A[illegible]		[illegible]	1%	6%	6%	0%	94%	[illegible]elefo[illegible]
18	A[illegible]		[illegible]	1%	0%	0%	0%	100%	[illegible]enije [illegible]
19	A[illegible]		[illegible]	1%	3%	3%	0%	97%	[illegible]ast Ca[illegible]
20	AS[illegible]		[illegible]	1%	3%	97%	0%	3%	[illegible]k Con[illegible]stinian Territory
21	A[illegible]		[illegible]	1%	3%	3%	0%	97%	[illegible]es Ltd.
22	A[illegible]		[illegible]	1%	3%	3%	0%	97%	[illegible]y Solu[illegible]
23	A[illegible]		[illegible]	1%	1%	1%	1%	99%	TELE2, SE, Sweden
24			[illegible]	1%	2%	2%	2%	96%	ELISA-AS Elisa Oyj, FI, Finland
25	A[illegible]		[illegible]	1%	0%	0%	0%	99%	TSF-IP-CORE TeliaSonera Finl[illegible]
			[illegible]	1%	5%	5%	5%	90%	Internet

% of clients who do not use Google's P-DNS

% of clients who appear to use DNSSEC-validating resolvers

% of clients who use Google's P-DNS and other resolvers

% of clients who use a mix of DNSSEC-validating resolvers and non-validating resolvers

% of clients who use non-validating resolvers

% of clients who exclusively use Google's P-DNS

Map client IP to origin AS, and select origin ASs with more than 500 data points

DNSSEC by Networks - the Top 25

Rank	ASN	Tests	DNSSEC Validation			Google P-DNS			
			Validating	Mixed	None	All	Mixed	None	
1	AS22047	5,376	98%	1%	1%	1%	0%	99%	VTR BANDA ANCHA S.A., CL, Chile
2	AS16232	1,818	98%	1%	1%	2%	0%	98%	ASN-TIM TIM (Telecom Italia Mobile) Autonomous System, IT, Italy
3	AS37457	2,051	97%	1%	2%	1%	0%	99%	Telkom-Internet, ZA, South Africa
4	AS39651	860	97%	1%	2%	1%	1%	98%	COMHEM-SWEDEN Com Hem Sweden, SE, Sweden
5	AS12912	613	96%	1%	2%	2%	0%	98%	ERA Polska Telefonia Cyfrowa S.A., PL, Poland
6	AS29562	1,263	95%	1%	4%	2%	1%	97%	KABELBW-ASN Kabel BW GmbH, DE, Germany
7	AS23944	749	94%	1%	5%	3%	1%	96%	SKYBB-AS-AP AS-SKYBroadband SKYCable Corporation, PH, Philippines
8	AS45629	8,759	94%	3%	4%	1%	1%	97%	JASTEL-NETWORK-TH-AP JasTel Network International Gateway, TH, Thailand
9	AS45758	15,833	93%	4%	3%	0%	2%	98%	TRIPLETNET-AS-AP TripleT Internet Internet service provider Bangkok, TH, Thailand
10	AS36925	1,012	93%	2%	5%	25%	1%	74%	ASMedi, MA, Morocco
11	AS7679	551	93%	1%	6%	1%	0%	99%	QTNET Kyushu Telecommunication Network Co., Inc., JP
12	AS6849	6,301	92%	3%	5%	5%	3%	92%	UKRTELNET JSC UKRTELECOM, , UA
13	AS34779	1,043	91%	3%	6%	2%	0%	98%	T-2-AS T-2, d.o.o., SI
14	AS198471	722	91%	4%	6%	95%	2%	4%	LINKEM-AS Linkem spa, IT, Italy
15	AS5466	1,463	90%	3%	6%	3%	1%	97%	EIRCOM Eircom Limited, IE, Ireland
16	AS28220	563	89%	2%	9%	5%	1%	94%	CABO SERVICOS DE TELECOMUNICACOES LTDA, BR, Brazil
17	AS5610	2,094	88%	3%	9%	6%	7%	87%	TO2-CZECH-REPUBLIC Telefonica Czech Republic, a.s., CZ
18	AS5603	1,505	88%	3%	9%	0%	1%	99%	SIOL-NET Telekom Slovenije d.d., SI, Slovenia
19	AS7922	43,438	87%	3%	9%	3%	1%	96%	COMCAST-7922 - Comcast Cable Communications, Inc., US
20	AS51737	753	87%	9%	4%	97%	2%	1%	SUPERLINK-AS SuperLink Communications Co, PS, Occupied Palestinian Territory
21	AS3249	1,093	84%	5%	10%	3%	1%	97%	ESTPAK Elion Enterprises Ltd., EE, Estonia
22	AS5645	1,993	83%	2%	14%	3%	0%	96%	TEKSAVVY-TOR TekSavvy Solutions Inc. Toronto, CA, Canada
23	AS1257	880	83%	1%	16%	1%	1%	99%	TELE2, SE, Sweden
24	AS719	655	82%	2%	16%	2%	2%	96%	ELISA-AS Elisa Oyj, FI, Finland
25	AS1759	1,080	82%	4%	15%	0%	0%	99%	TSF-IP-CORE TeliaSonera Finland IP Network, FI, Finland
		5,331,072	**7%**	**5%**	**88%**	**5%**	**5%**	**90%**	**Internet**

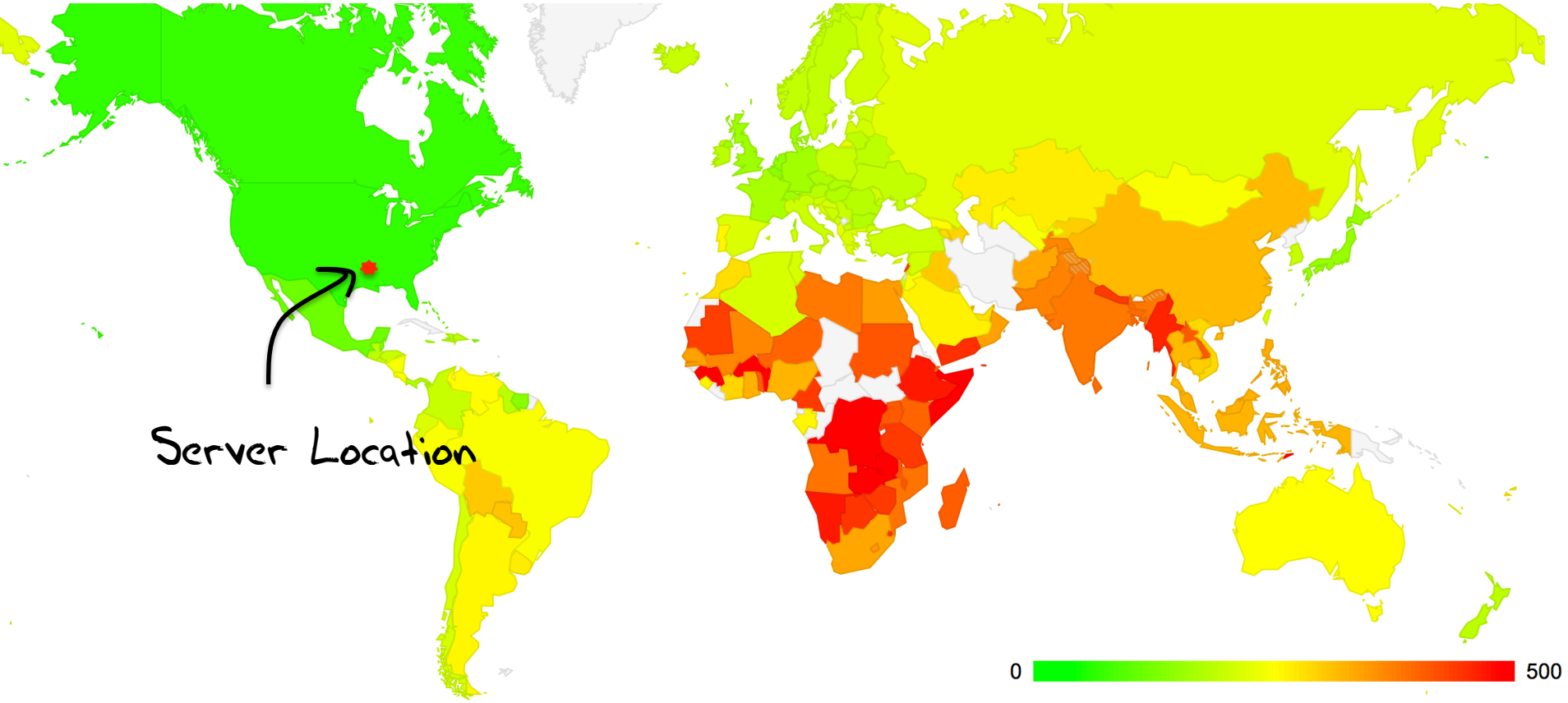
Map client IP to origin AS, and select origin ASs with more than 500 data points

DNS Performance

How can we measure the time taken to resolve each of the three DNSSEC domain name types (signed, unsigned, badly signed)?

2. DNSSEC Performance

Absolute Measurements don't make much sense…



Average RTT from Client to Server by country of origin (ms)

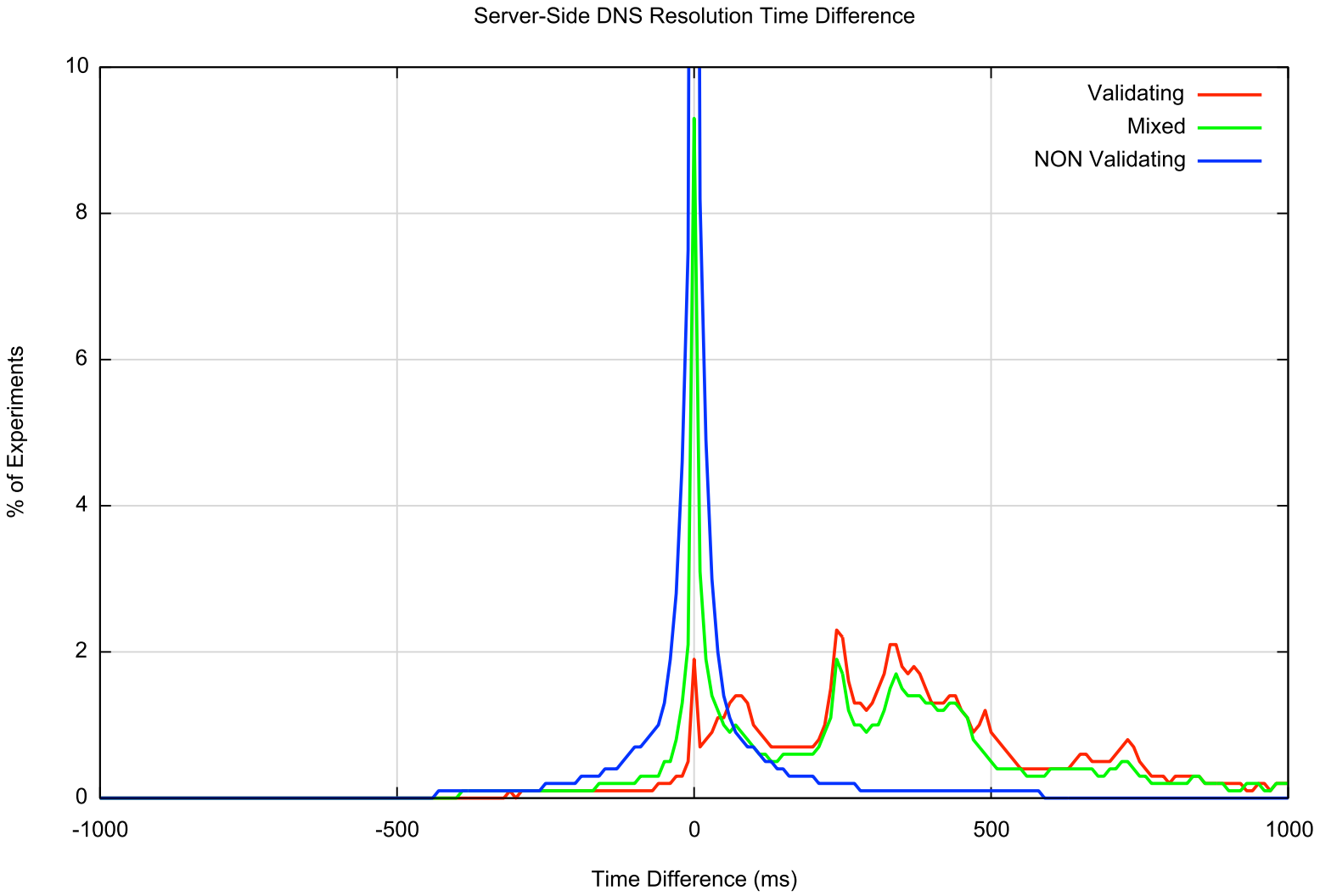
Relative Measurements …

Let's define the FETCH TIME as the time at the authoritative server from the first DNS query for an object to the HTTP GET command for the same object

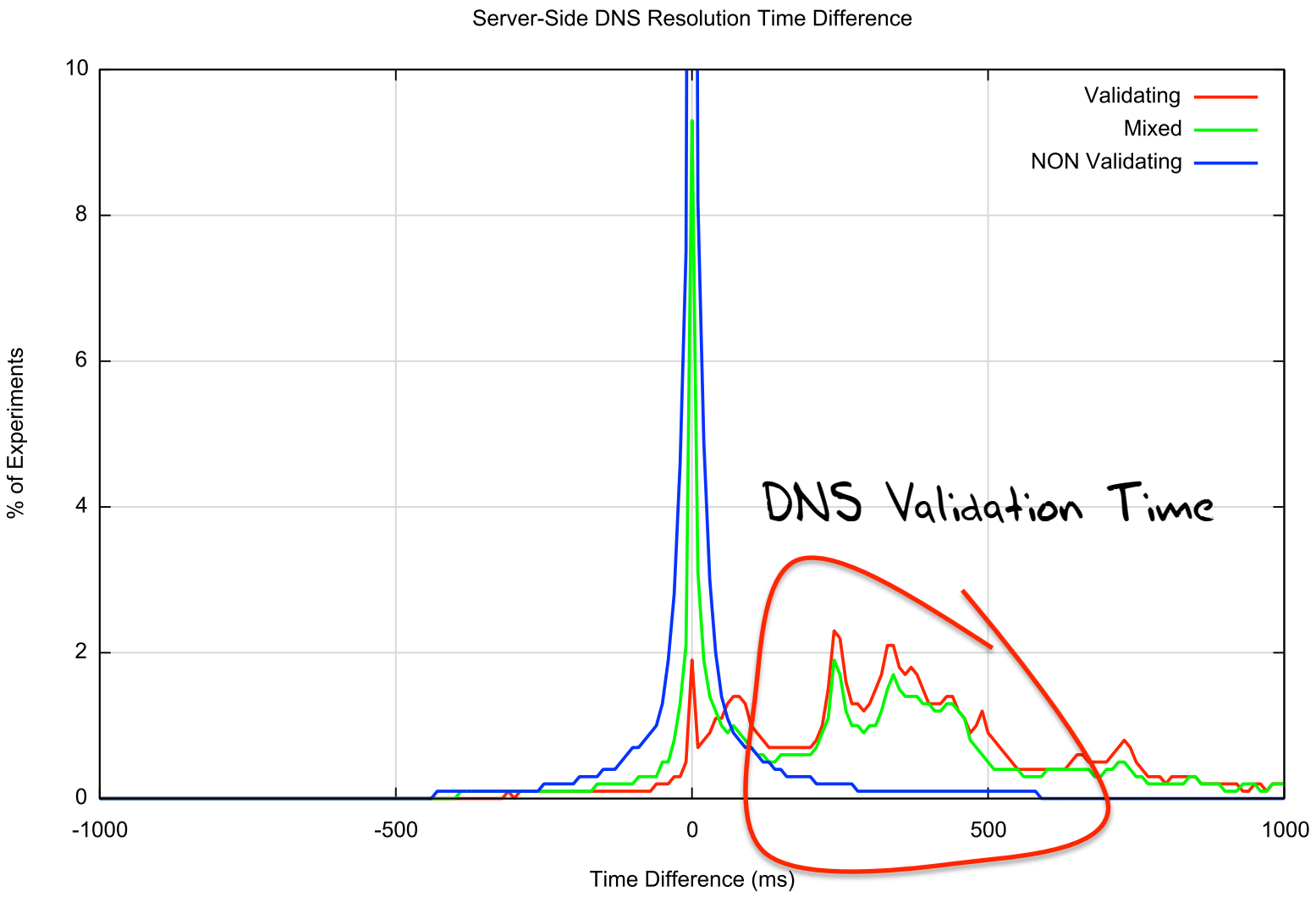
- This time should reflect the DNS resolution time and a single RTT interval for the TCP handshake

If the "base" fetch time is the time to load an unsigned DNSSEC object, then how much longer does it take to load an object that is DNSSEC-signed?

Result

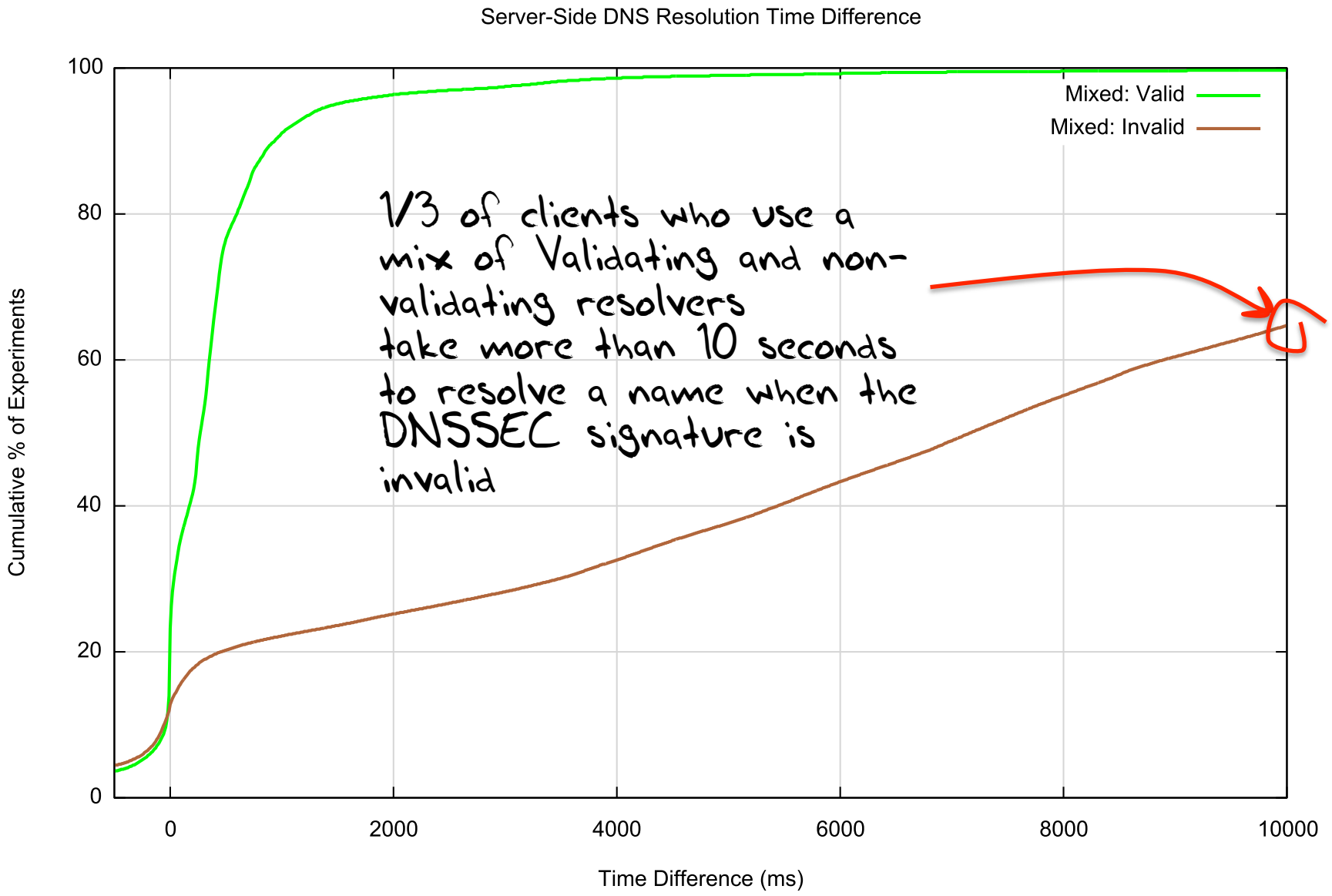

Server-Side DNS Resolution Time Difference
% of Experiments
Time Difference (ms)
Validating
Mixed
NON Validating
10
8
6
4
2
0
-1000
-500
0
500
1000

Result


Server-Side DNS Resolution Time Difference
Validating
Mixed
NON Validating
DNS Validation Time
% of Experiments
Time Difference (ms)
10
8
6
4
2
0
-1000
-500
0
500
1000

Invalid DNSSEC Signature

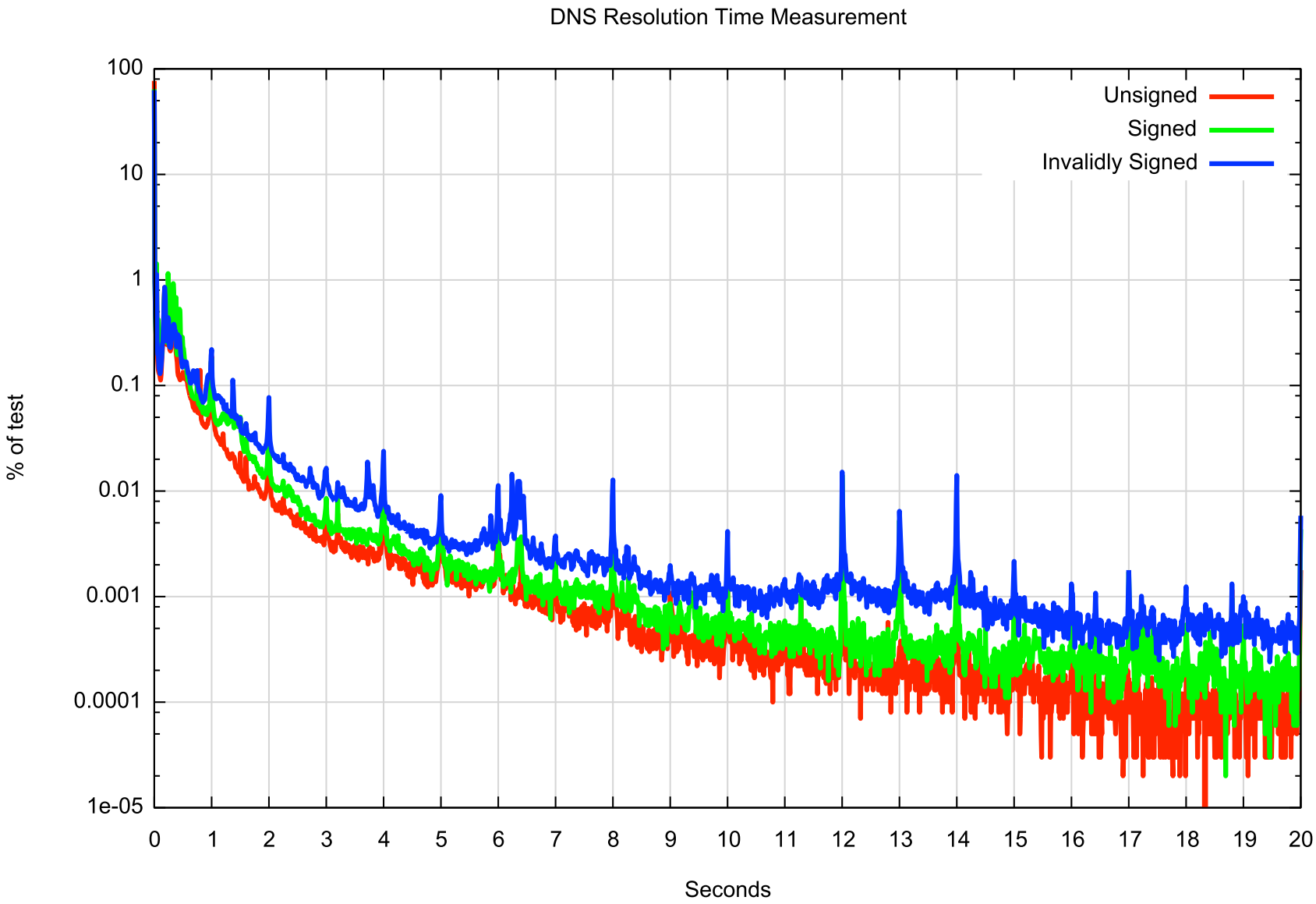
Invalid DNSSEC Signature



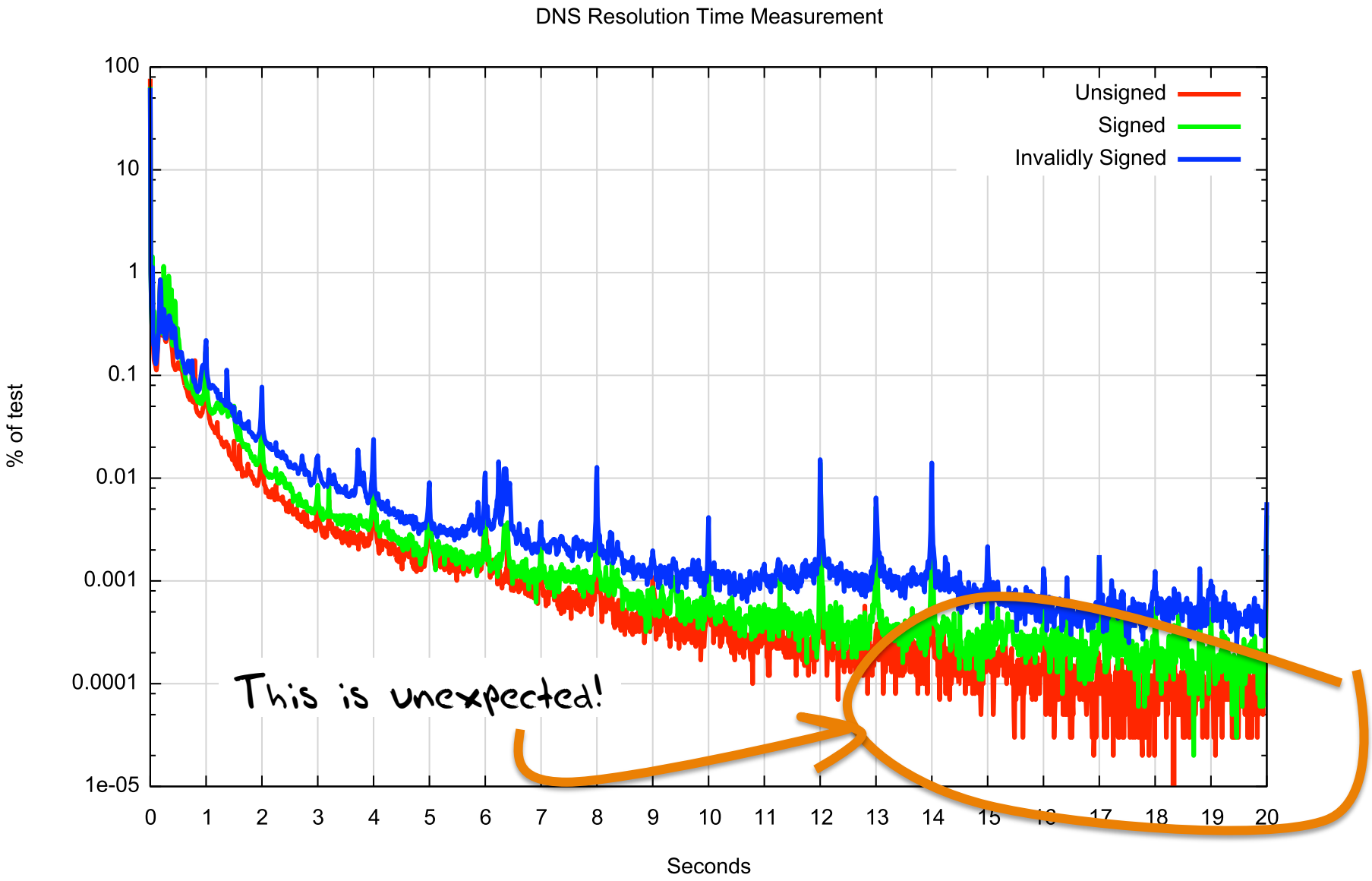
DNS Query Time

Now let's look at the elapsed time at the DNS server between the first query for a name and the last query

DNS Query Time



DNS Query Time



What can we say?

DNSSEC takes longer

- Which is not a surprise
- Additional queries for DS and DNSKEY RRs
- At a minimum that's 2 DNS query/answer intervals
  - Because it appears that most resolvers serialise and perform resolution then validation

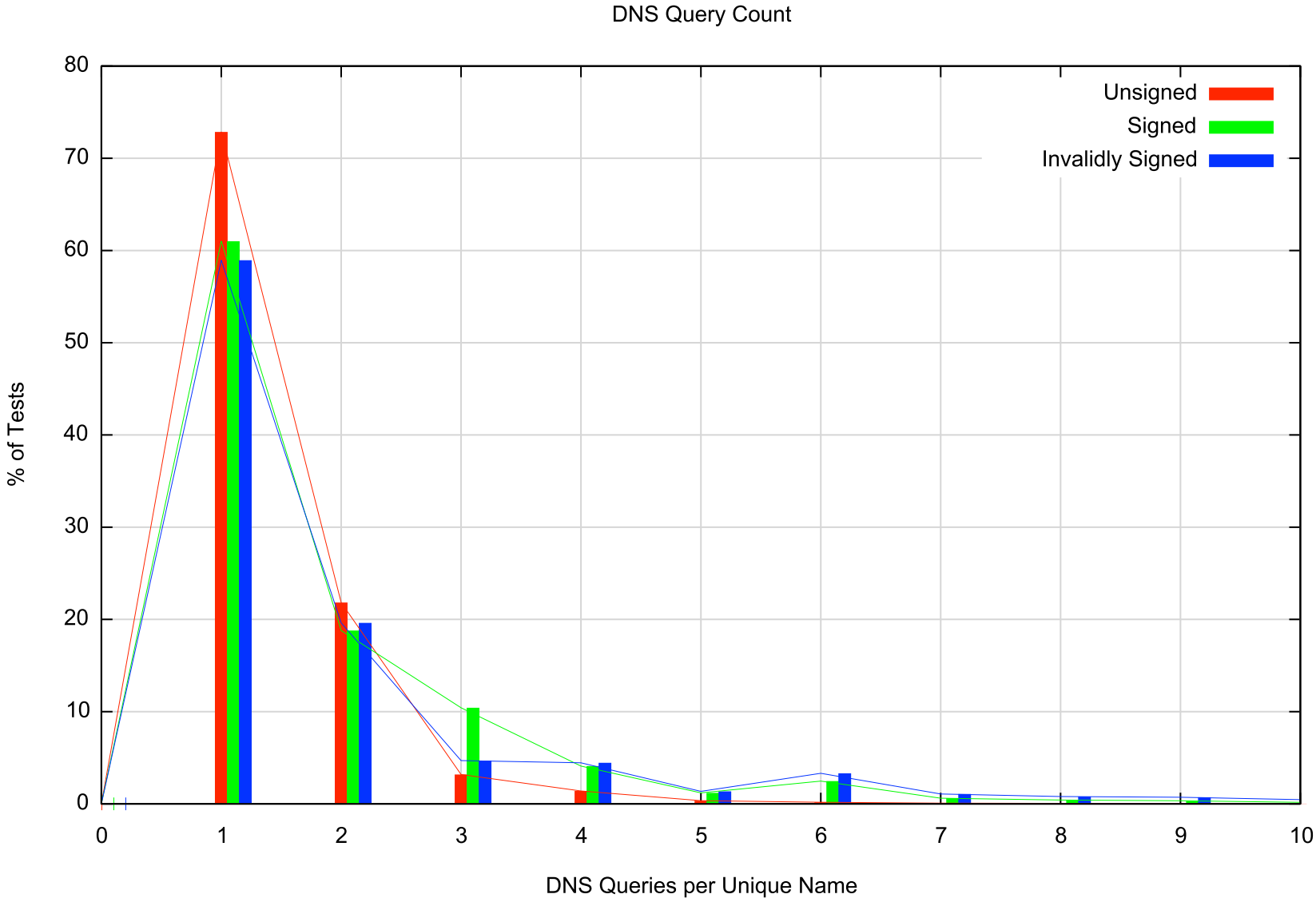
Badly-Signed DNSSEC takes even longer

- Resolvers try hard to find a good validation path
- And the SERVFAIL response causes clients to try subsequent resolvers in their list

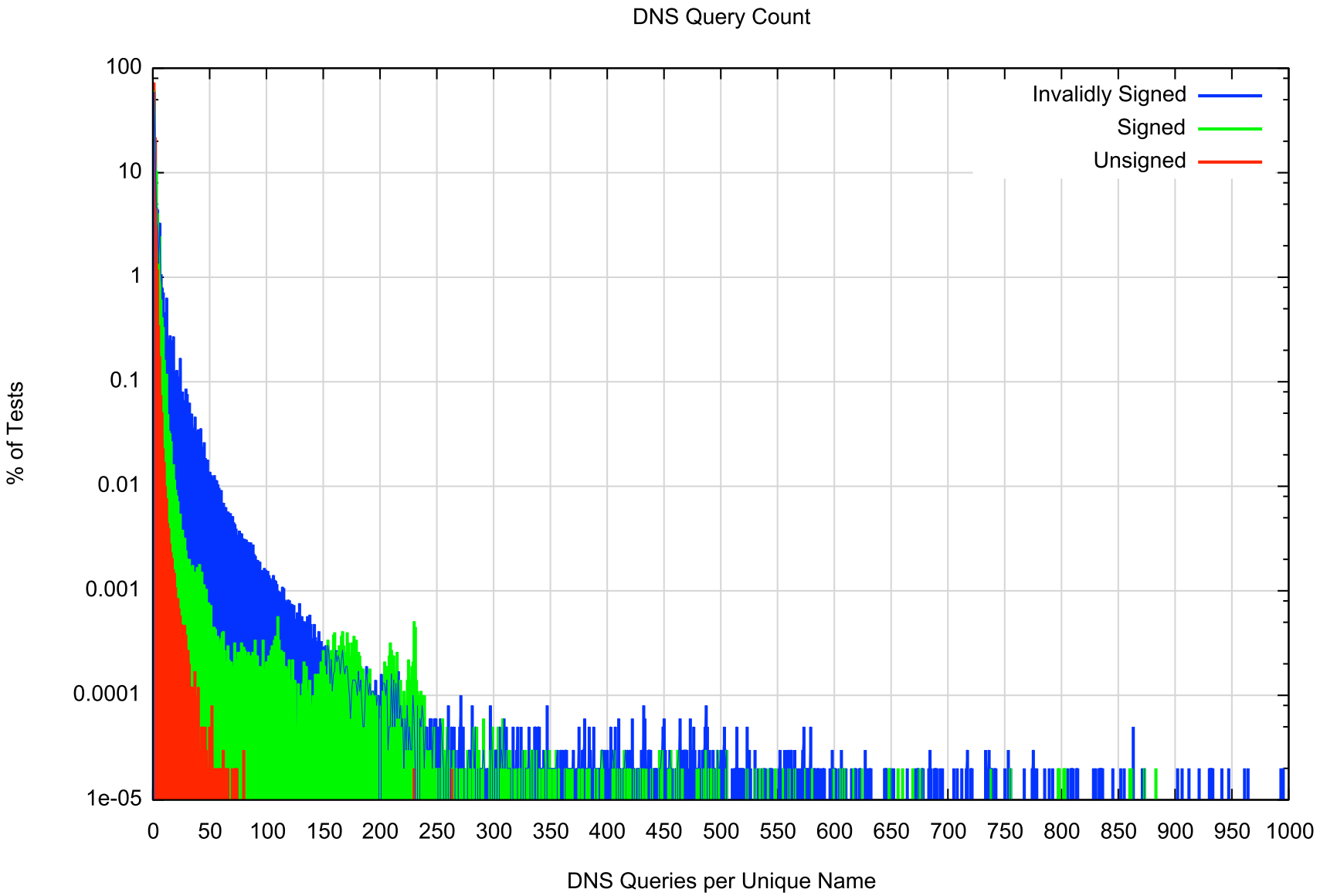
3. At the other end…

Let's look at performance from the perspective of an Authoritative Name server who serves DNSSEC-signed domain names

DNS Query count per Domain Name



DNS Query count per Domain Name



DNSSEC Performance

At the Authoritative Name Server:

Serving DNSSEC-signed zones = More Queries!

- The Authoritative server will now see additional queries for the DNSKEY and DS RRs for a zone, in addition to the A (and AAAA) queries

6,095,289 launched experiments

8,367,427 unsigned name queries

12,375,232 signed name queries

20,130,781 badly-signed name queries

What if everybody was doing it?

For the control name there are 1.4 queries per experiment

The total profile of queries for the control DNS name was:

7.4M A queries

0.7M AAAA queries

0.2M Other (NS, MX, ANY, SOA, CNAME, TXT, A6) queries

For the signed name, only 11.4% of clients use DNSSEC-aware resolvers, so the theory (2 additional queries per name) says we will see 1.4M additional queries, or 9.8M queries in total

But we saw 12.4 M queries for the signed DNS Name

- If 11.5% of clients' resolvers using DNSSEC generate an additional 4.0M queries for a signed domain name, what if every DNS resolver was DNSSEC aware?
- That would be 35M queries in the context of our experiment

A DNSSEC signed zone would see ~4 times the query level of an unsigned zone if every resolver performed DNSSEC validation

Good vs Bad for Everyone

If 12.6% of clients performing some form of DNSSEC validation generate 20.1M queries for a badly-signed name, compared to the no-DNSSEC control level of 8.4M queries, what would be the query load if every resolver performed DNSSEC validation for the same badly signed domain?

- In our case that would be 102M queries

A badly-signed DNSSEC signed zone would seen 12 times the query level of an unsigned zone if every resolver performed DNSSEC validation

Response Sizes

What about the relative traffic loads at the server?

In particular, what are the relative changes in the traffic profile for responses from the Authoritative Server?

DNS Response Sizes

Control (no DNSSEC)

Query: 124 octets
Response: 176 octets

DNSSEC-Signed

Query: (A Record) 124 octets
Response: 951 Octets

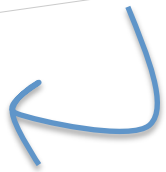
Query: (DNSKEY Record) 80 octets
Response: 342 Octets

Query: (DS Record) 80 octets
Response: 341 Octets

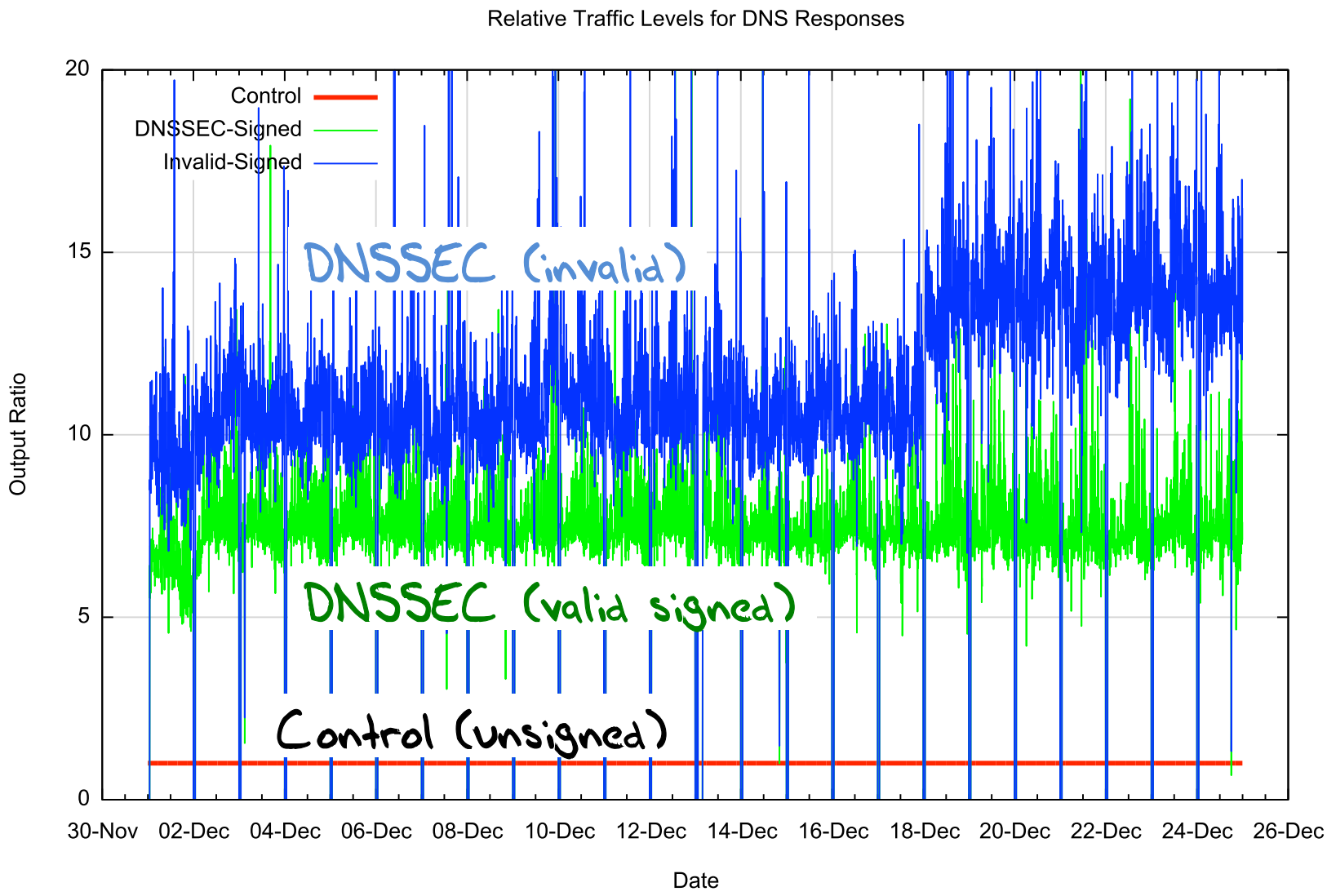
Total: Query: 284 octets
Total Response: 1634 octets

These are not constant sizes – the DNS packet sizes of responses relate to the particular name being resolver, the number of keys being used, and the key size

So these numbers are illustrative of what is going on, but particular cases will vary from these numbers



Measurement - Response Traffic Volume



Interpreting Traffic Data

The validly-signed domain name appears to generate 8x the DNS response traffic volume, as compared to the unsigned domain name

The badly-signed domain name appears to generate 10x – 14x the DNS response traffic volume

What's contributing to this?

1. Setting the DNSSEC OK bit in a query to the signed zone raises the response size from 176 to 951 octets
2. Performing DNSSEC signature validation adds a minimum of a further 683 octets in DS and DNSKEY responses

What if you just sign your domain?

Lets start with the hypothetical question: How much more traffic will you be generating at the Authoritative Server if you sign your domain and NO resolvers perform DNSSEC validation?

84% of A and AAAA queries seen at the authoritative nameserver have the EDNS0 + DNSSEC OK flags set

- 81.5% of queries for the unsigned zone
- 83.3% of queries for the signed zone
- 85.9% of queries for the badly-signed zone

(aside: why are these proportions different for each of these zones?)

If you just sign your zone and NO resolvers are performing DNSSEC validation

- 84% of queries elicit the larger DNS response then the total outbound traffic load is **4.7x** the traffic load of an unsigned zone

But we saw a rise of **8x** – why?

- That's because 12.6 % of clients are also performing DNSSEC validation in various ways

What if everybody was doing it?

If 12.6% of clients performing some form of DNSSEC validation for a signed zone generate around 8x the traffic as compared to an unsigned zone, then what if every DNS resolver performed DNSSEC validation?

An authoritative server for a DNSSEC signed zone would see some 13 times the traffic level of an unsigned zone if every resolver performed DNSSEC validation

A badly-signed DNSSEC zone would see some 31 times the traffic level of an unsigned zone

DNSSEC means more Server Grunt

It's probably a good idea to plan to serve the worst case: a badly signed zone

In which case you may want to consider provisioning the authoritative name servers with processing capacity to handle **15x** the query load, and **30x** the generated traffic load that you would need to serve the unsigned zone when signing the zone

A Couple of Caveats:

Reality could be better than this…

"Real" performance of DNSSEC could be a lot better than what we have observed here

- We have deliberately negated any form of resolver caching
  - Every client receives a "unique" signed URL, and therefore every DNS resolver has to to perform A, DS and DNSKEY fetches for the unique label
  - The Ad placement technique constantly searches for "fresh eyeballs", so caching is not as efficient as it could be
  - Conventional DNS caching would dramatically change this picture
    - Our 16 day experiment generated 12,748,834 queries
    - A 7 day TTL would cut this to a (roughly estimated) 2M queries

And it could be a whole lot worse!

- For the invalid DNSSEC case we deliberately limited the impact of invalidity on the server
  - DNSSEC invalidity is not handled consistently by resolvers
  - Some resolvers will perform an exhaustive check of all possible NS validation paths in the event of DNSSEC validation failure

    See "Roll Over and Die" (http://www.potaroo.net/ispcol/2010-02/rollover.html)

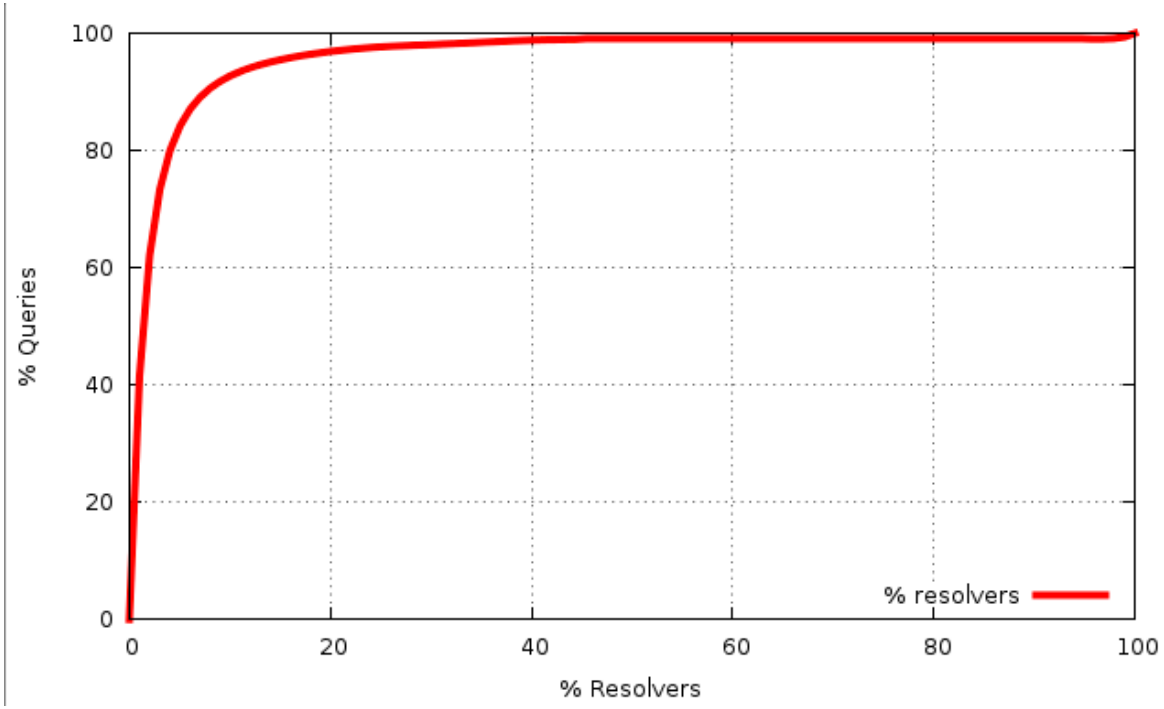
  - In this experiment we used a single NS record for the invalidly signed domains
  - If we had chosen to use multiple nameservers, or used a deeper-signed label path, or both, on the invalid label, then the query load would've been (a lot?) higher

- Resolver caching of invalidly signed data is also unclear – so a break in the DNSSEC validation material may also change the caching behaviour of resolvers, and increase load at the server

Some things to think about

Resolver / Client Distribution

- 1% of visible resolvers provide the server with 58% of the seen queries
- A few resolvers handle a very significant proportion of the total query volume
- But there are an awful lot of small, old, and poorly maintained resolvers running old code out there too!

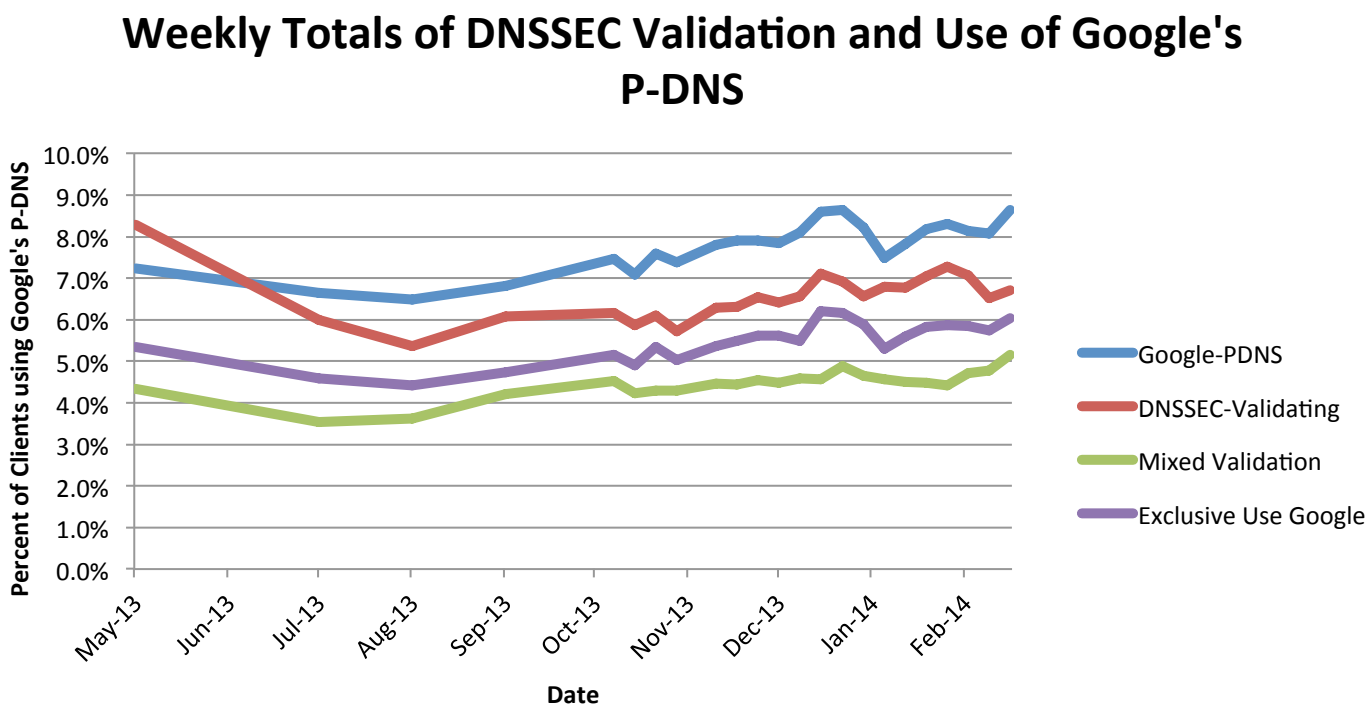


Some things to think about

- Google's Public DNS is currently handling queries from ~10% of the Internet's end client population
  - That's around 1 in 12 users
  - In this time of heightened awareness about corporate and state surveillance, and issues around online anonymity and privacy, what do we think about this level of use of Google's Public DNS Service?

Some things to think about

- Google's Public DNS is currently handling queries from 8% of the Internet's end client populat
  - That's
  - In this corpo aroun think DNS S



Some things to think about

Is the DNS borked?

Why do 20% of clients use resolvers that make >1 DNS query for a simple unsigned uncached domain name?

- Is the DNS resolver ecosystem THAT broken that 1 in 5 clients use resolvers that generate repeat queries gratuitously?
- And is it reasonable that 1 in 20 clients take more than 1 second to resolve a simple DNS name?

Some things to think about

- Why do some 84% of queries have EDNS0 and the DNSSEC OK flag set, yet only 6% of clients perform DNSSEC validation?
- How come we see relatively more queries with the DNSSEC OK flag set for queries to domains in signed zones?

Some things to think about

SERVFAIL is not just a “DNSSEC validation is busted” signal

- clients start walking through their resolver set asking the same query
- Which delays the client and loads the server
  - The moral argument: Failure should include a visible cost!
  - The expedient argument: nothing to see here, move along!

Maybe we need some richer signaling in the DNS for DNSSEC validation failure

Thanks!