

Measuring DNSSEC Use

Geoff Huston
APNIC Labs



We all know...

What DNSSEC does

And why it's a Good Thing to sign your DNS zones using DNSSEC

But's that's a "supply side" activity.

What about the demand side?

If you sign it will they validate?

Lets look at the world of DNSSEC from the end user's perspective

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?

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

On to Some 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%	4.5%	28.2%	Sweden
3	SI	5,883	51.0%	6.1%	42.9%	Slovenia
		2,112	44.7%	4%	50.9%	tonia
		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	21,167	26.6%	8%	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 non-validating resolvers

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

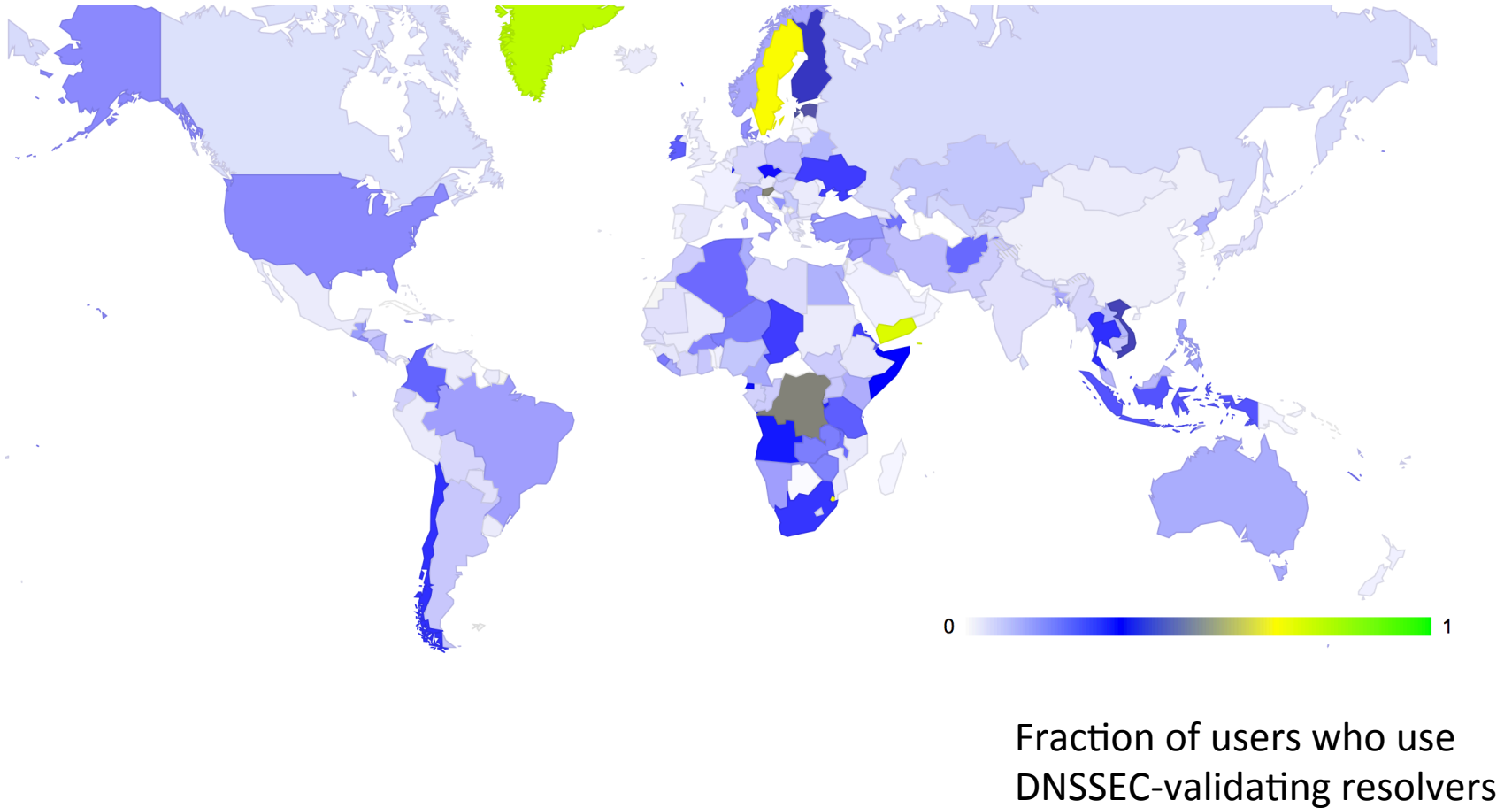
Rank	CC Code	Tests	Validating (%)	Mixed (%)	None (%)	
97	CN	1,215,241	1.9%	2.1%	96.0%	China
98	SA	45,243	1.7%	2.1%	96.2%	Saudi Arabia
99	MD	3,168	1.6%	1.9%	96.5%	Republic of Moldova
100	FR	86,888	1.6%	1.0%	97.4%	France
101	NZ	31,683	1.6%	15.0%	83.4%	New Zealand
102	BE	15,243	1.5%	3.8%	94.7%	Belgium
103	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

Most importantly...

Rank	CC Code	Tests	Validating	Mixed	None	Country
35	AU	22,173	10.72	2.68	86.6	Australia
101	NZ	31,683	1.57	15.04	83.39	New Zealand

The Mapped view of DNSSEC Use



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 Online Security Blog

The latest news and insights from Google on security and safety on the Internet

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?

Rank	CC Code	DNSSEC Validation		Google Public DNS			
		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
			1.1%	5.0%	4%	94.7%	Slovenia
			1.0%	4.2%	1%	94.8%	Poland
			2.4%	98.7%	0.3%	99.1%	Yemen
			1.0%	2.1%	0.8%	97.1%	Yemen
			0.8%	13.8%	0.5%	85.7%	Yemen
			9.8%	15.9%	0.8%	83.3%	Yemen
			6.8%	15.9%	5.9%	78.4%	Yemen
10	CL	21,167	26.6%	15.9%	0.4%	83.7%	Chile
11	ZA	12,167	26.6%	15.9%	0.4%	83.7%	South Africa
12	UA	32,167	26.6%	15.9%	0.4%	83.7%	Ukraine
13	ID	89,167	26.6%	15.9%	0.4%	83.7%	Indonesia
14	IE	7,167	26.6%	15.9%	0.4%	83.7%	Ireland
15	TZ	1,167	26.6%	15.9%	0.4%	83.7%	Tanzania
16	CO	25,167	26.6%	15.9%	0.4%	83.7%	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?

Rank	CC Code	DNSSEC Validation		Google Public DNS			
		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?

Rank	CC Code	DNSSEC Validation		Google Public DNS			
		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			Google P-DNS			AS Name	
		Validating	Mixed	None	All	Mixed	None		
1	AS22047	5,376	98%	1%	1%	1%	0%	99%	VIP
2	AS16232	1,818	98%	1%	1%	2%	0%	98%	ASN-TIM TIM (Telecom Italia Mobile) Autonomous Syst
			97%	1%	2%	1%	0%	99%	ikom-Internet, ZA, South Africa
			97%	1%	2%	1%	1%	98%	COMHEM SWEDEN Com Hem Sweden, SE, Sweden
			96%	1%	2%	1%	0%	96%	ERA Polska Telekomunikacji S.A., PL, Poland
			95%	1%	4%	1%	1%	97%	KABELBW-ASN Kabel BW, DE, Germany
			94%	1%	5%	3%	1%	96%	SKYBB-AS-AP AS-SKYBroad
			94%	1%	4%	1%	1%	97%	JASTEL NETWORK-TH-AP JasTel Net
			93%	1%	3%	0%	1%	98%	TRIPLET-AS-AP TripleT Internet Intern
			93%	1%	5%	25%	1%	74%	ASMedi, MA, Morocco
			93%	1%	6%	1%	1%	99%	QTNET Kyushu Communication Netwo
			92%	1%	5%	5%	1%	92%	UKRTELNET JSC UKRTELNET, UA
13	AS34779	1,043	91%	1%	6%	2%	1%	96%	T-2-AS T-2, d.o.o., SI
14	AS198471	722	91%	1%	6%	95%	2%	95%	LINKEM-AS Linkem spa, IT, Italy
15	AS5466	1,463	91%	1%	6%	3%	1%	96%	TELECOM IRELAND, IE, Ireland
16	AS28220	562	91%	1%	0%	5%	1%	93%	TELECOMUNICACAOES BRASILEIRAS S.A. - B3, BR, Brazil
17	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
18	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
19	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
20	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
21	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
22	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
23	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
24	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
25	AS198471	722	91%	1%	6%	95%	2%	95%	TELECOM IRELAND, IE, Ireland
			91%	1%	6%	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 Telefonii 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 SKY Cable 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

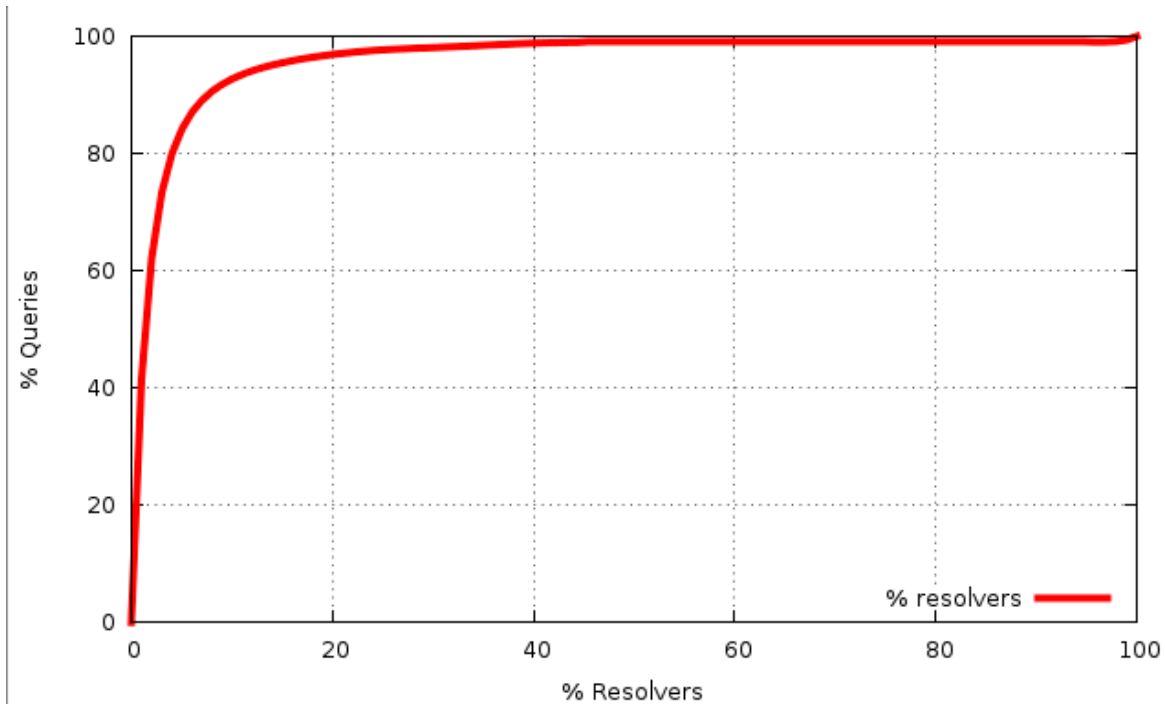
Some things to think about

- DNSSEC generates very large responses from very small queries
 - Which makes it a highly effective DDOS amplifier
 - Is relying on BCP38 going to work?
 - Do we need to think about DNS over TCP again?
 - But how many resolvers/firewalls/other middleware stuff support using TCP for DNS?
 - What's the impact on the authoritative server load and caching recursive resolver load when moving from UDP to TCP?

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 ~8% 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 popula

popula

– That

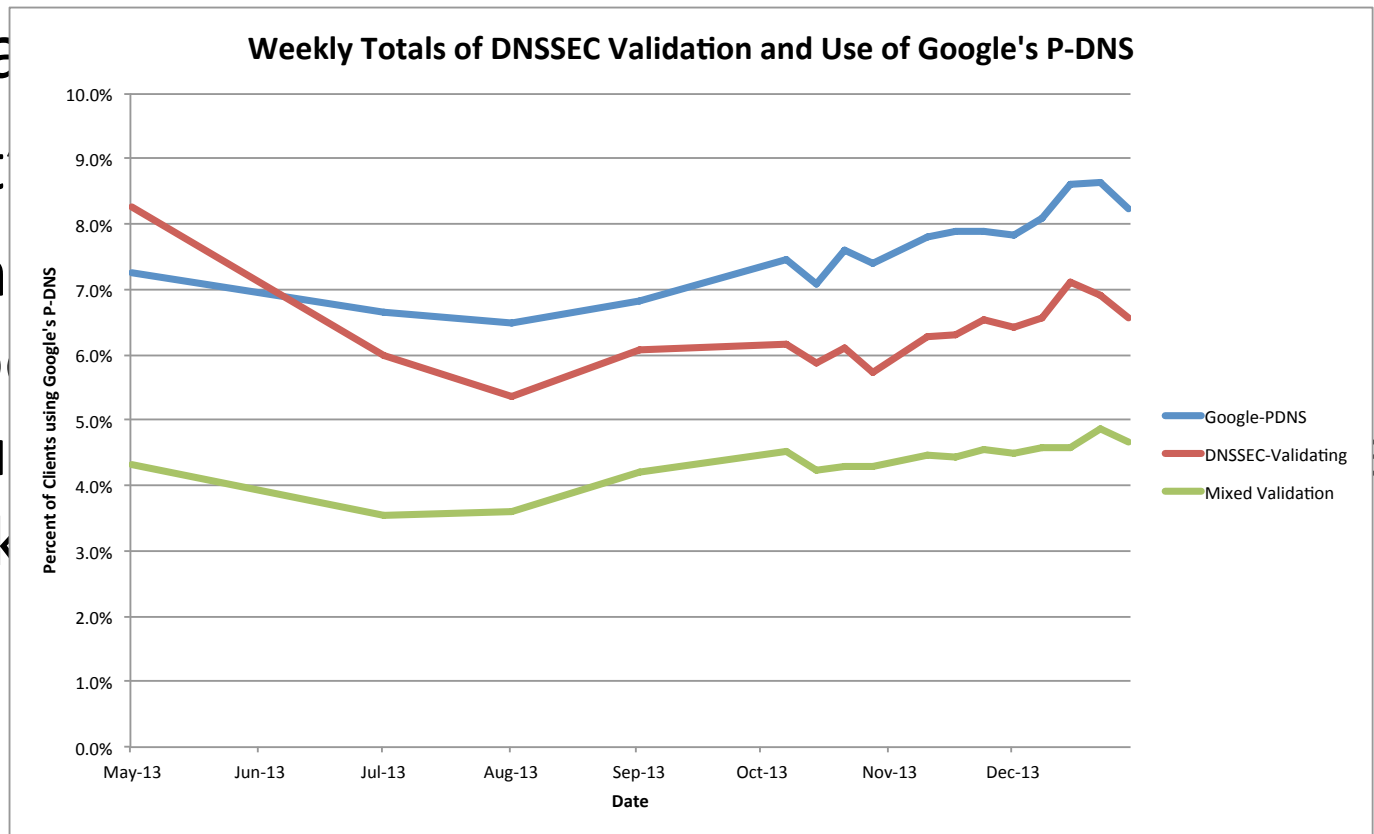
– In th

corp

arou

think

DNS



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

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?

Thanks!