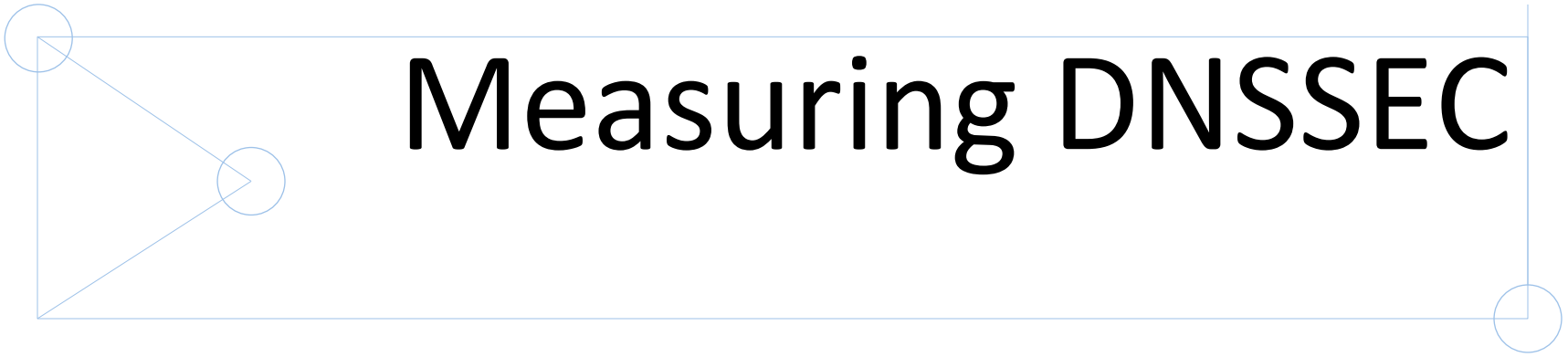


Measuring DNSSEC

Geoff Huston
APNIC Labs,
June 2014

Users vs Infrastructure

- We often measure the network by observing infrastructure and inferring end user behaviour
  - because it's often easier to instrument infrastructure
- This is aimed at measuring an aspect of of behaviour within particular parameters of the network infrastructure, but it does not encompass how the end user assembles a coherent view of available services

Measuring Users

- Seed a user with a set of tasks that cause identifiable traffic at an instrumented server
- The server performs the measurement

Measuring DNSSEC via Ads

Client is given 4 URLs to load:

- DNSSEC-validly signed DNS name
- DNSSEC-invalidly signed DNS name
- Unsigned DNS name (control)
- Result reporting URL (10 second timer)

These URLs use a unique signed name component to circumvent DNS caching, and ensure that all DNS queries ultimately are passed to the authoritative server for the name

On to Some Results

90 days: March to May 2014

- Presented: 69,068,769 experiments

Web + DNS query log results for clients:

- Performed DNSSEC signature validation and did not fetch the invalidly signed object: **9.6%**
- Fetched DNSSEC RRs, but then retrieved the invalidly signed object anyway: **5.3%**
- Did not have a DNSSEC clue at all - only fetched A RRs: **85.1%**

Where is DNSSEC? – The Top 20

Rank	CC	Tests	Validating	Mixed	Not	
1	SE	37,684	72.98%	4.08%	22.94%	Sweden
2	YE	6,400	66.78%	9.[illegible]8%	23.8[illegible]	Yemen
3	SI	56,1[illegible]	55.50%	6.[illegible]3%	38.27%	Slovenia
4			55.33%	5[illegible]%	39.47%	Estonia
5			51.06%	6[illegible]%	42[illegible]	[illegible]buda
6			45.36%	7[illegible]%	46[illegible]	
7			44.69%	1[illegible]%	42[illegible]	
8			41.46%	1[illegible]%	39[illegible]	
9		[illegible]	41.21%	[illegible]	52[illegible]	
10	CZ	104,307			54[illegible]	
11	PL	281,979			58.33%	Poland
12	BB	7,601			65.36%	Barbados
13	CO	1,010,663			66.07%	Colombia
14	FJ	2,898			43.20%	Fiji
15	FI	25,556			67.47%	Finland
16	GH	11,979			46.82%	Ghana
17	LU	3,993			62.43%	Luxembourg
18	NC	1,599	25.77%	6.44%	67.79%	New Caledonia
19	IE	19,418	24.88%	3.69%	71.43%	Ireland
20	ZA	18,885	24.49%	7.30%	68.21%	South Africa
	XA	69537051	9.57%	6.67%	83.31%	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	Tests	Validating	Mixed	Not	
1	SE	37,684	72.98%	4.08%	22.94%	Sweden
2	YE	6,400	66.78%	9.38%	23.84%	Yemen
3	SI	56,148	55.50%	6.23%	38.27%	Slovenia
4	EE	30,926	55.33%	5.20%	39.47%	Estonia
5	AG	2,362	51.06%	6.90%	42.04%	Antigua and Barbuda
6	DK	17,499	45.36%	7.71%	46.93%	Denmark
7	VN	974,737	44.69%	13.00%	42.31%	Vietnam
8	IQ	145,345	41.46%	18.81%	39.73%	Iraq
9	RO	556,795	41.21%	5.81%	52.98%	Romania
10	CZ	104,307	34.13%	10.98%	54.90%	Czech Republic
11	PL	281,979	33.21%	8.46%	58.33%	Poland
12	BB	7,601	32.89%	1.75%	65.36%	Barbados
13	CO	1,010,663	31.38%	2.55%	66.07%	Colombia
14	FJ	2,898	30.06%	26.74%	43.20%	Fiji
15	FI	25,556	29.79%	2.74%	67.47%	Finland
16	GH	11,979	29.09%	24.09%	46.82%	Ghana
17	LU	3,993	27.15%	10.42%	62.43%	Luxembourg
18	NC	1,599	25.77%	6.44%	67.79%	New Caledonia
19	IE	19,418	24.88%	3.69%	71.43%	Ireland
20	ZA	18,885	24.49%	7.30%	68.21%	South Africa
	XA	69537051	9.57%	6.67%	83.31%	World

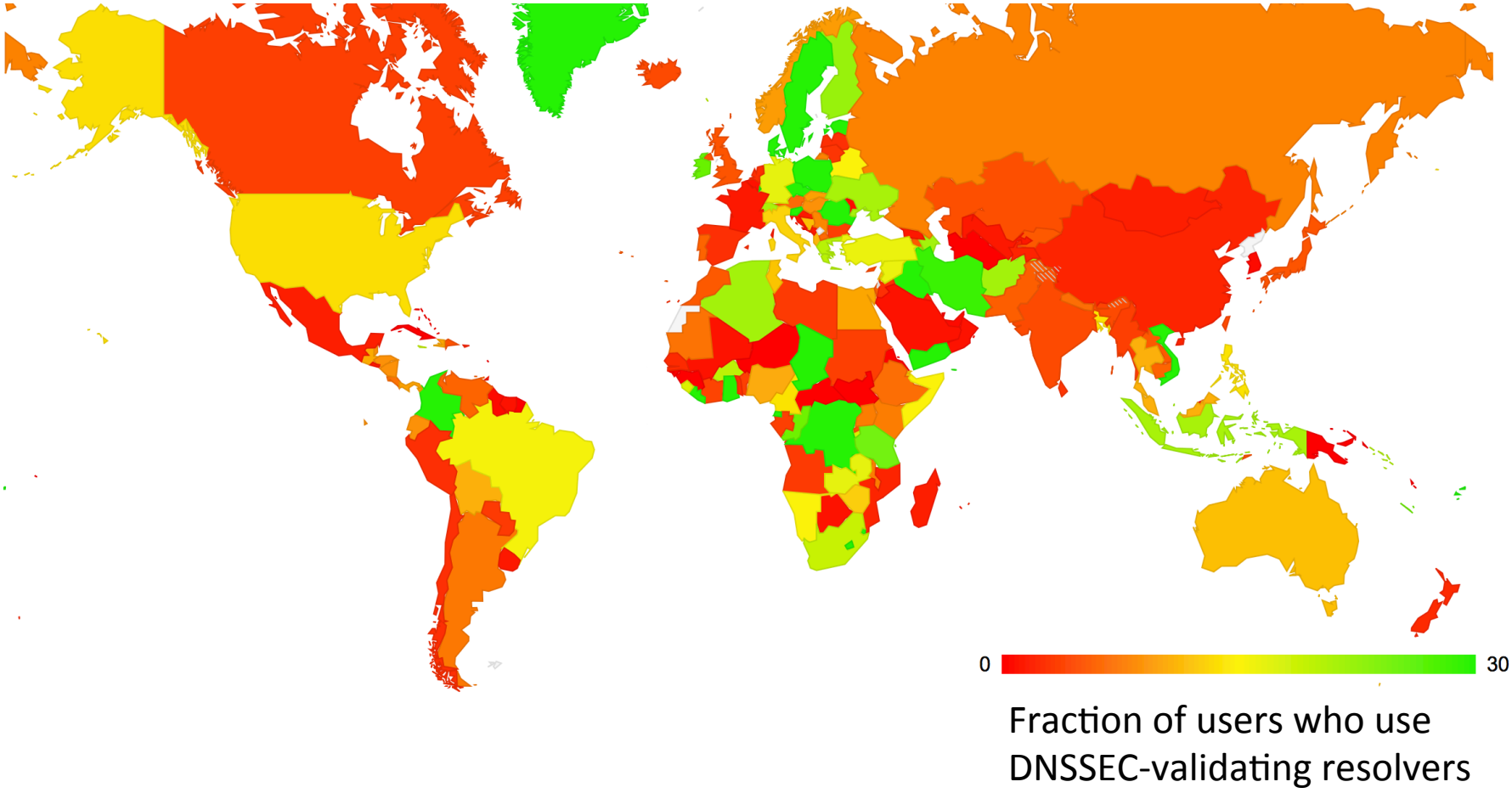
Geo-locate clients to countries, and select countries with more than 1,000 data points

Where isn't DNSSEC? – The Bottom 20

Rank	CC	Tests	Validating	Mixed	Not	
137	SD	2,699	1.78%	14.60%	83.62%	Sudan
138	FR	288,310	1.67%	1.17%	97.16%	France
139	MG	3,442	1.66%	2.15%	96.19%	Madagascar
140	SR	8,031	1.64%	2.00%	96.35%	Suriname
141	UY	50,811	1.64%	0.89%	97.47%	Uruguay
142	BE	42,603	1.54%	4.37%	94.09%	Belgium
143	ML	2,585	1.51%	1.70%	96.79%	Mali
144	JO	24,101	1.50%	2.34%	96.16%	Jordan
145	MD	32,599	1.49%	1.57%	96.94%	Republic of Moldova
146	SA	209,493	1.47%	1.41%	97.12%	Saudi Arabia
147	OM	21,954	1.42%	2.18%	96.40%	Oman
148	SG	155,692	1.36%	3.72%	94.92%	Singapore
149	HR	101,390	1.35%	0.93%	97.72%	Croatia
150	GY	3,579	1.12%	0.25%	98.63%	Guyana
151	TJ	5,819	1.01%	0.96%	98.02%	Tajikistan
152	BS	4,985	0.80%	1.00%	98.19%	Bahamas
153	AE	126,771	0.78%	1.19%	98.03%	United Arab Emirates
154	PF	3,877	0.67%	0.93%	98.40%	French Polynesia
155	KR	534,274	0.47%	0.96%	98.57%	Republic of Korea
156	QA	58,229	0.45%	0.89%	98.65%	Qatar
	XA	69,537,051	9.57%	6.67%	83.31%	World

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

The Mapped view of DNSSEC Use

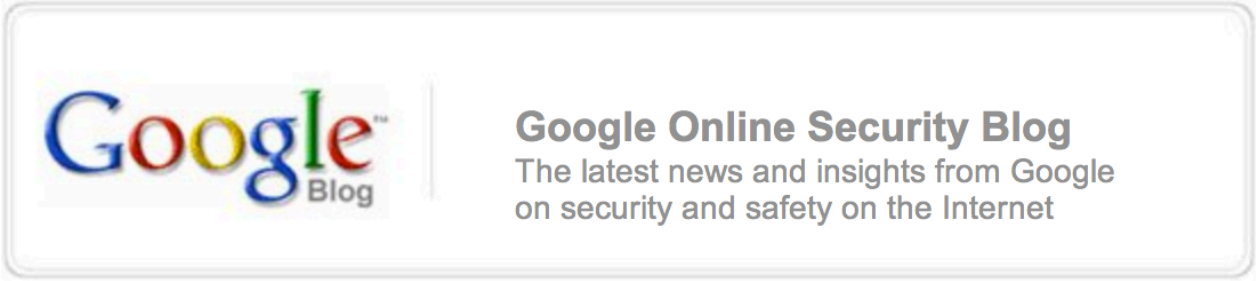


http://gronggrong.rand.apnic.net/cgi-bin/worldmap (June 2014)

Why…

is it that 9.6**%** of users performing DNSSEC validation is about 4 times the number of users who are capable of using IPv6?

Is Google's P-DNS a Factor?



Google Public DNS Now Supports DNSSEC Validation

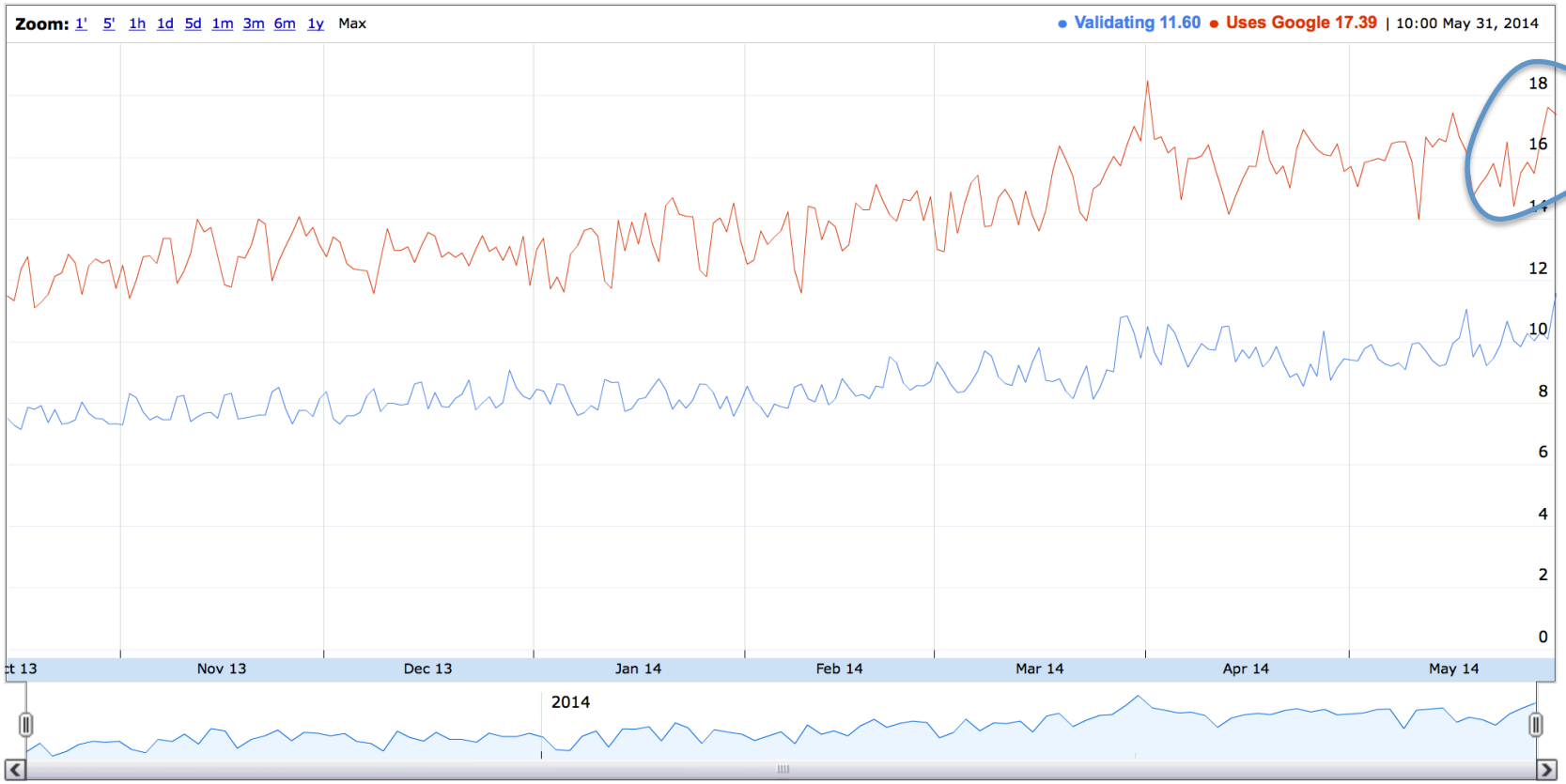
Tuesday, March 19, 2013 8:30 AM
Posted by Yunhong Gu, Team Lead, Google Public DNS

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: **16%**



Is Google's P-DNS a Factor?

Rank	CC	Tests	Validating	Mixed	Not	Google	
1	SE	37,684	72.98%	4.08%	22.94%	[illegible]%	Sweden
2	YE	6,400	66.78%	9.38%	23.84%	12.92%	Yemen
3	SI	56			[illegible]%	7.04%	Slovenia
4	EE	30			[illegible]47%	3.82%	Estonia
5	AG	2			42.04%	9.95%	Antigua and Barbuda
6	DK	17			46.93%	6.56%	Denmark
7	VN	974			42.31%	59.37%	Vietnam
8	IQ	145			39.73%	34.62%	Iraq
9	RO	556			52.98%	6.19%	Romania
10	CZ	104,307	34.13%	10.98%	54.90%	16.07%	Czech Republic
11	PL	281,979	33.21%	8.46%	58.33%	10.15%	Poland
12	BB	7,601	32.89%	1.75%	65.36%	3.38%	Barbados
13	CO	1,010,663	31.38%	2.55%	66.07%	6.39%	Colombia
14	FJ	2,898	30.06%	26.74%	43.20%	30.40%	Fiji
15	FI	25,556	29.79%	2.74%	67.47%	2.17%	Finland
16	GH	11,979	29.09%	24.09%	46.82%	31.33%	Ghana
17	LU	3,993	27.15%	10.42%	62.43%	10.47%	Luxembourg
18	NC	1,599	25.77%	6.44%	67.79%	10.51%	New Caledonia
19	IE	19,418	24.88%	3.69%	71.43%	7.59%	Ireland
20	ZA	18,885	24.49%	7.30%	68.21%	10.01%	South Africa
	XA	69,537,051		9.57%	6.67%	83.31%	15.72% World

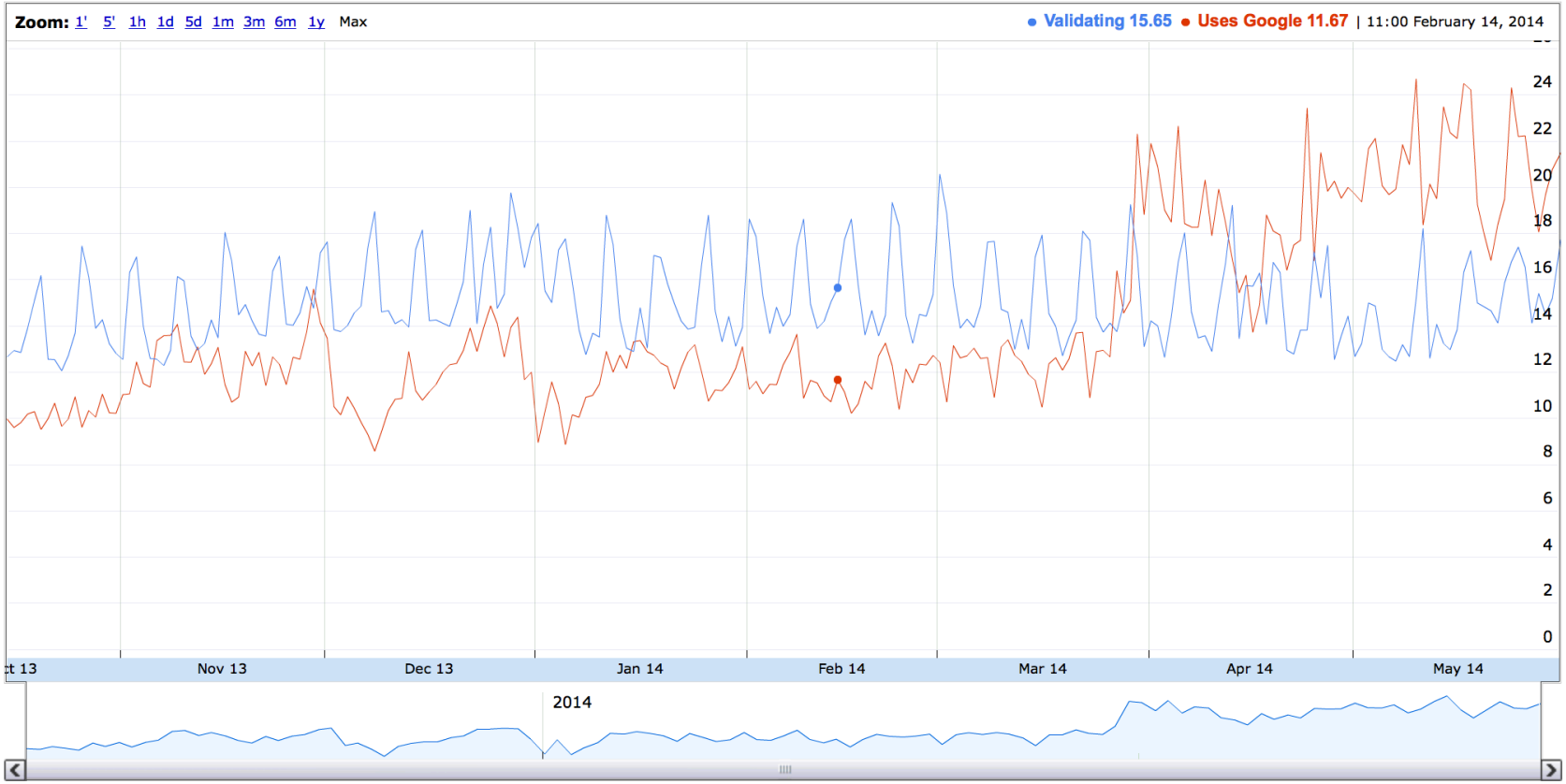
% of end users who have their queries passed to Google's P-DNS Service

Is Google's P-DNS a Factor?

Rank	CC	Tests	Validating	Mixed	Not	Google	
1	SE	37,684	72.98%	4.08%	22.94%	5.00%	Sweden
2	YE	6,400	66.78%	9.38%	23.84%	12.92%	Yemen
3	SI	56,14Ω	55.50%	6.23%	38.27%	7.04%	Slovenia
4	EE	30,926	55.33%	5.20%	39.47%	3.82%	Estonia
5	AG	2,362	51.06%	6.90%	42.04%	9.95%	Antigua and Barbuda
6	DK	17,499	45.36%	7.71%	46.93%	6.56%	Denmark
7	VN	974,737	44.69%	13.00%	42.31%	59.37%	Vietnam
8	IQ	145,345	a1.46%	18.81%	39.73%	34.62%	Iraq
9	RO	556,795	41.21%	5.81%	52.98%	6.19%	Romania
10	CZ	104,307	34.13%	10.98%	54.90%	16.07%	Czech Republic
11	PL	281,979	33.21%	8.46%	58.33%	10.15%	Poland
12	BB	7,601	32.89%	1.75%	65.36%	3.38%	Barbados
13	CO	1,010,663	31.38%	2.55%	66.07%	6.39%	Colombia
14	FJ	2,898	30.06%	26.74%	43.20%	30.40%	Fiji
15	FI	25,556	29.79%	2.74%	67.47%	2.17%	Finland
16	GH	11,979	29.09%	24.09%	46.82%	31.33%	Ghana
17	LU	3,993	27.15%	10.42%	62.43%	10.47%	Luxembourg
18	NC	1,599	25.77%	6.44%	67.79%	10.51%	New Caledonia
19	IE	19,418	24.88%	3.69%	71.43%	7.59%	Ireland
20	ZA	18,885	24.49%	7.30%	68.21%	10.01%	South Africa
	XA	69,537,051		9.57%	6.67%	83.31%	15.72% World

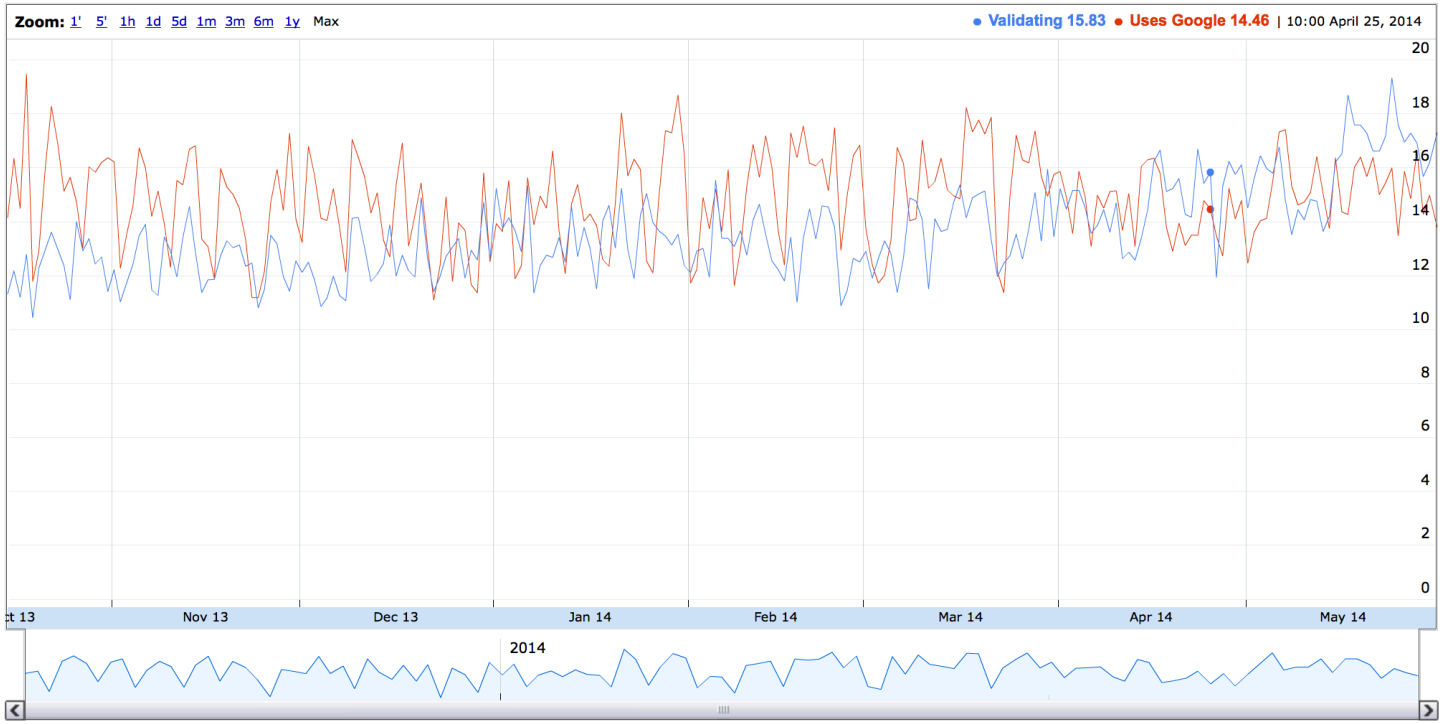
A DNSSEC view of the US

DNSSEC Country Deployment for United States of America (US)



http://gronggrong.rand.apnic.net/cgi-bin/ccpage?c=US

DNSSEC Country Deployment for Brazil (BR)

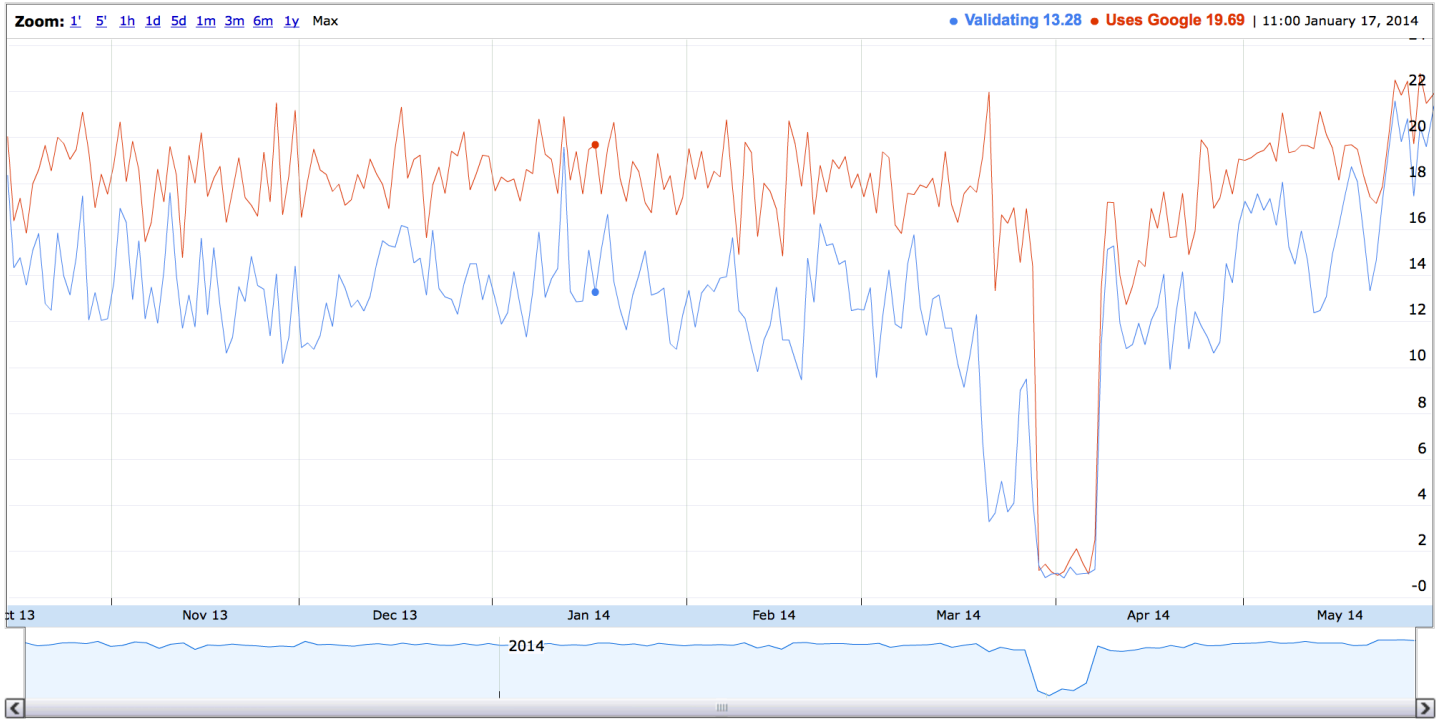


World Map of DNSSEC Deployment

ASN	AS Name	DNSSEC Validates	Uses Google PDNS	Samples
AS28573	NET Servios de Comunicao S.A.	21.71%	4.47%	105755
AS18881	Global Village Telecom	11.23%	16.12%	88847
AS7738	Telemar Norte Leste S.A.	7.86%	10.60%	72883
AS27699	TELEFNICA BRASIL S.A	3.09%	4.53%	57258
AS8167	Brasil Telecom SA - Filial Distrito Federal	9.84%	13.28%	45749
AS13591	Brasil Telecom Comunicao Multimidia	1.49%	6.13%	23530
AS53006	COMPANHIA DE TELECOMUNICACOES DO BRASIL CENTRAL	5.60%	7.33%	6820
AS26599	TELEFNICA BRASIL S.A	1.15%	2.38%	6090
AS4230	EMBRATEL-EMPRESA BRASILEIRA DE TELECOMUNICAES SA	30.62%	45.89%	4589
AS26615	Tim Celular S.A.	5.68%	14.10%	3822

Meanwhile, in Turkey…

DNSSEC Country Deployment for Turkey (TR)



World Map of DNSSEC Deployment

ASN	AS Name	DNSSEC Validates	Uses Google PDNS	Samples
AS9121	TTNET Turk Telekomunikasyon Anonim Sirketi	12.51%	16.05%	587394
AS34984	TELLCOM-AS TELLCOM ILETISIM HIZMETLERI A.S.	14.69%	18.96%	74938
AS47331	TTNET TTNet A.S.	13.10%	15.76%	56072
AS12978	DOGAN-ONLINE DOGAN TV DIGITAL PLATFORM ISLETMECILIGI A.S.	15.03%	18.06%	29792
AS47524	TURKSAT-AS Turksat Uydu Haberlesme ve Kablo TV Isletme A.S.	15.05%	18.27%	25106
AS8517	ULAKNET National Academic Network and Information Center	12.04%	32.14%	11192
AS16135	TURKCELL-AS TURKCELL ILETISIM HIZMETLERI A.S.	3.29%	4.79%	6740
AS8386	KOCNET VODAFONE NET ILETISIM HIZMETLERI A.S	15.52%	19.84%	6677
AS12735	ASTURKNET TurkNet Iletisim Hizmetleri A.S	41.80%	19.55%	5811
AS20978	AVEA-TELEKOMUNIKASYON AVEA Iletisim Hizmetleri A.S.	6.76%	10.97%	4350

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?

    Results from October 2013: 84% of resolvers, 94% of users
  - 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

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?

Some things to think about

- Google's Public DNS is currently handling queries from ~16% of the Internet's end client population
  - That's around 1 in 6 users

Google Announcement

|< | < Prev | Random | Next > | >|

|< | < Prev | Random | Next > | >|

Permanent link to this comic: http://xkcd.com/1361/
Image URL (for hotlinking/embedding): http://imgs.xkcd.com/comics/google_announcement.png

```
$ dig +short TXT google-public-dns-a.google.com
"http://xkcd.com/1361/"
```

http://gronggrong.rand.apnic.net/cgi-bin/worldmap

Thanks

APNIC Labs:

Geoff Huston research@apnic.net