Measuring the DNS from the Users' perspective

Geoff Huston
APNIC Labs,
May 2014

What's the question?

How many users can do <x> with the DNS?

- How many users can retrieve a URL using IPv6?
- How many users perform DNSSEC validation when they resolve a domain name?
- How many users are capable of resolving a name via DNS over TCP?
- How many users follow DNAME chains in the DNS?

etc

Users vs Infrastructure

- We often measure the network by observing infrastructure and inferring end user behaviour
  - because its often easier to instrument infrastructure
- This approach 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 the network

For example…DNSSEC

- We can walk zone files and count the number of signed zones
- Or we could analyze the log files of authoritative name servers for a signed zone and attempt to infer something about the number of users who use DNSSEC to validate DNS responses
- But can these sort of approaches measure the population of end users who are served by DNSSEC-validating resolvers?

How to measure a million end users

How to measure a million end users

- Be Google (or any other massively popular web service provider)

How to measure a million end users

- Be Google (or any other massively popular web service provider)

or

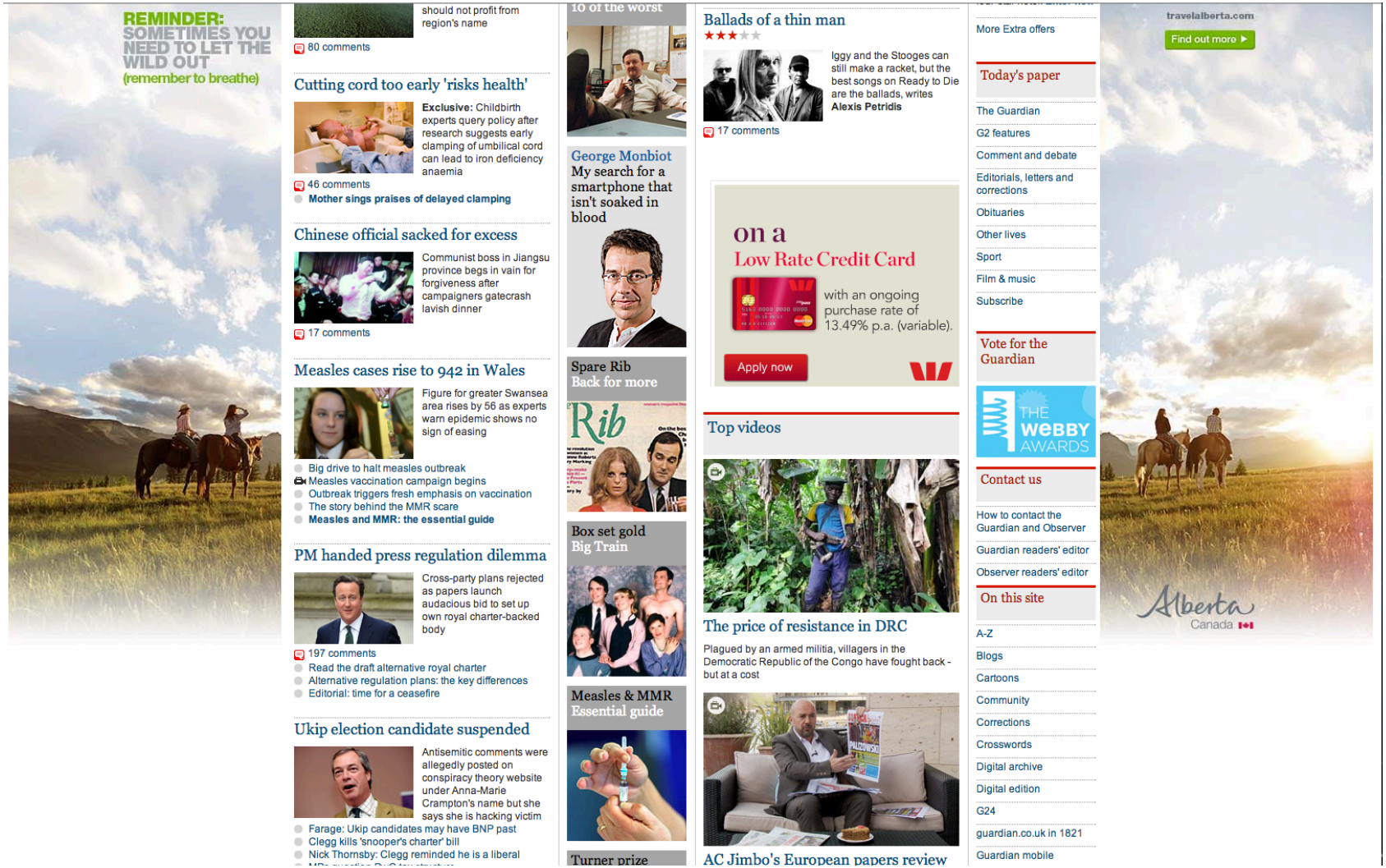
How to measure a million end users

- Be Google (or any other massively popular web service provider)

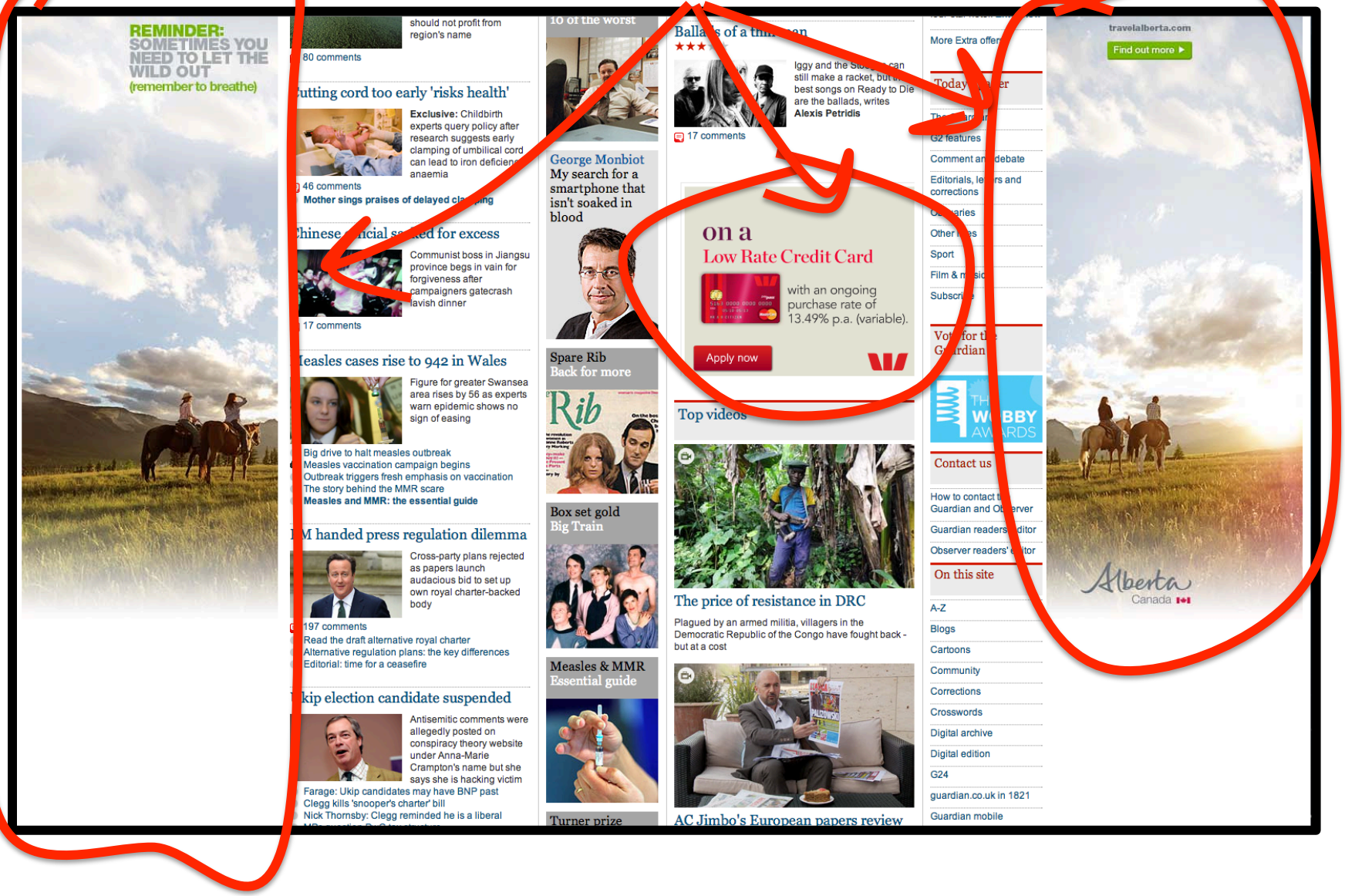
or

- Get your code to run on a million users' machines through another delivery channel

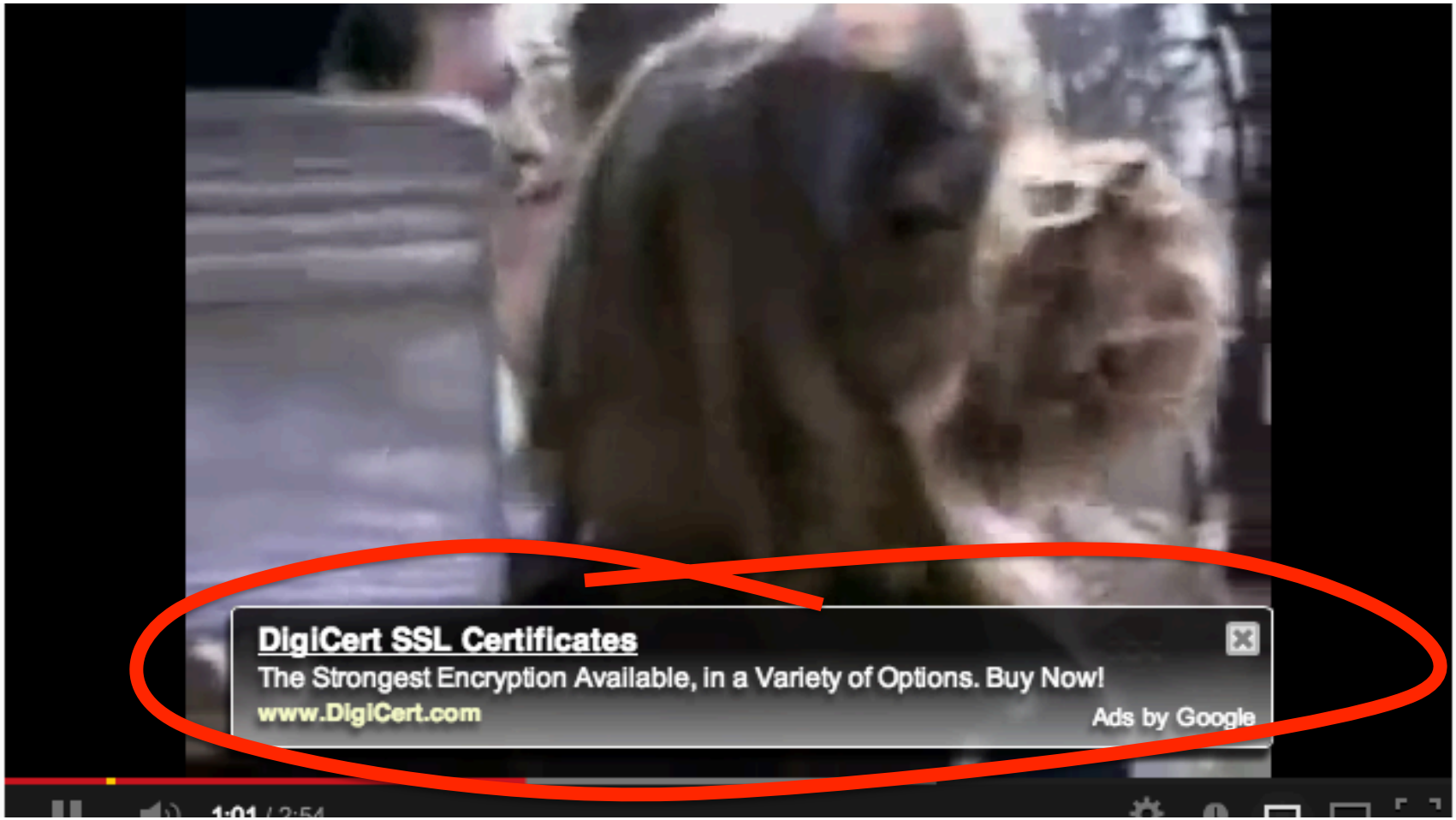
Ads are ubiquitous



Ads are ubiquitous



Ads are ubiquitous



Ads are implemented in Adobe Flash

- Flash includes primitives in ‘actionscript’ to fetch ‘network assets’
  - Typically used to load alternate images, sequences
  - Not a generalized network stack, subject to constraints:
    - Port 80
    - crossdomain.xml on hosting site must match source name (wildcard syntax)
- Flash has asynchronous ‘threads’ model for event driven, sprite animation

APNIC's measurement technique

- Craft flash/actionscript which fetches network assets to measure when the ad is displayed
- Web Assets are reduced to a notional '1x1' image which is not added to the DOM and is not displayed
- Assets can be named to cause specific DNS resolution via local gethostbyname() styled API within the browser's Flash engine
- Encode data transfer in the name of fetched assets
  - Use the DNS as the information conduit:
    - Result is returned by DNS name with wildcard
  - Use HTTP as the information conduit
    - Result is returned via parameters attached to an HTTP GET command

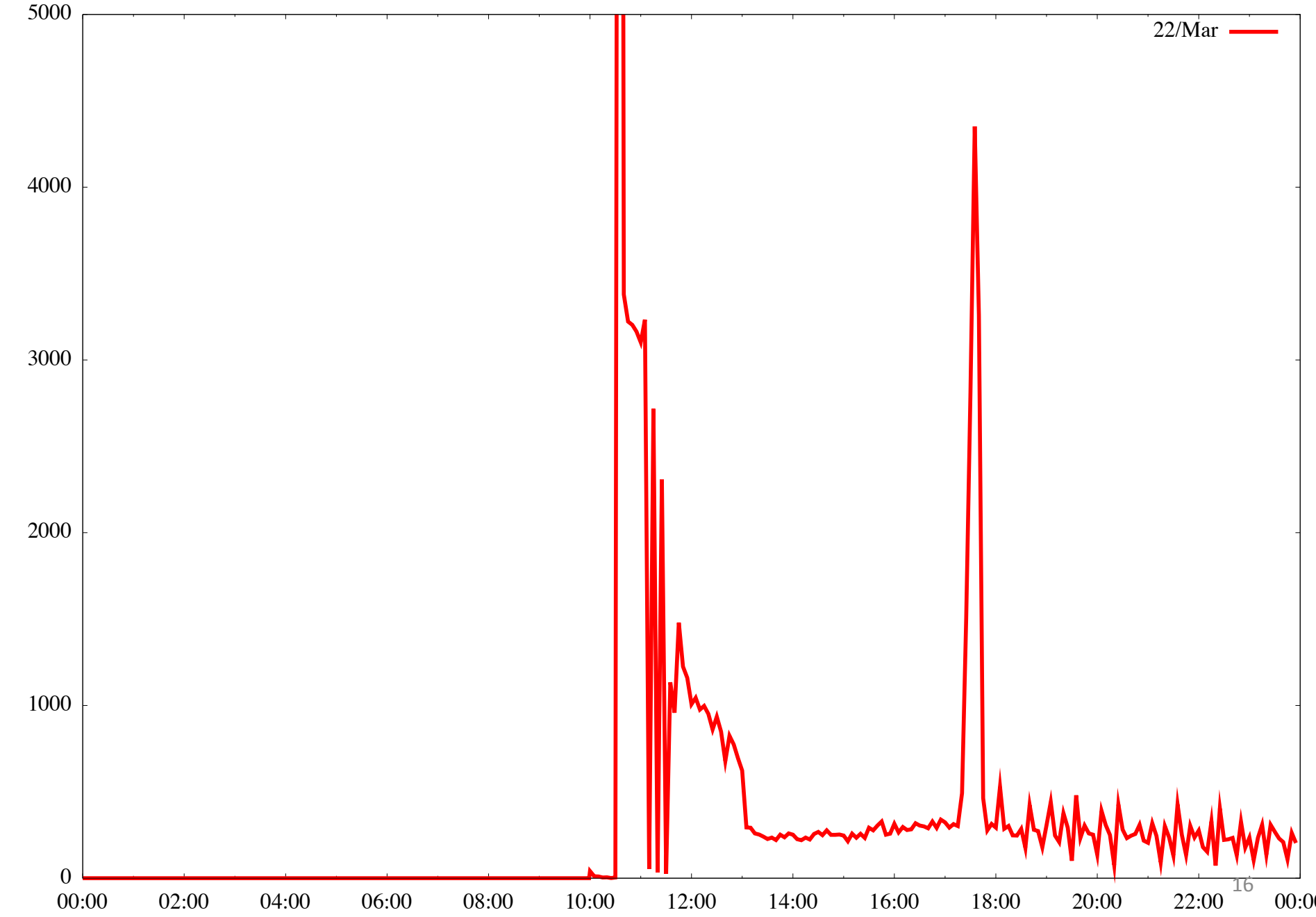
Advertising placement logic

- Fresh Eyeballs == Unique IPs
  - We have good evidence the advertising channel is able to sustain a constant supply of unique IP addresses
- Pay by click, or pay by impression
  - If you select a preference for impressions, then the channel tries hard to present your ad to as many unique IPs as possible
- Time/Location/Context tuned
  - Can select for time of day, physical location or keyword contexts (for search-related ads)
  - But if you don't select, then placement is generalized
- Aim to fill budget
  - If you request $100 of placement a day, then inside 24h algorithm tries hard to even placement but in the end, will 'soak' place your ad to achieve enough views, to bill you $100

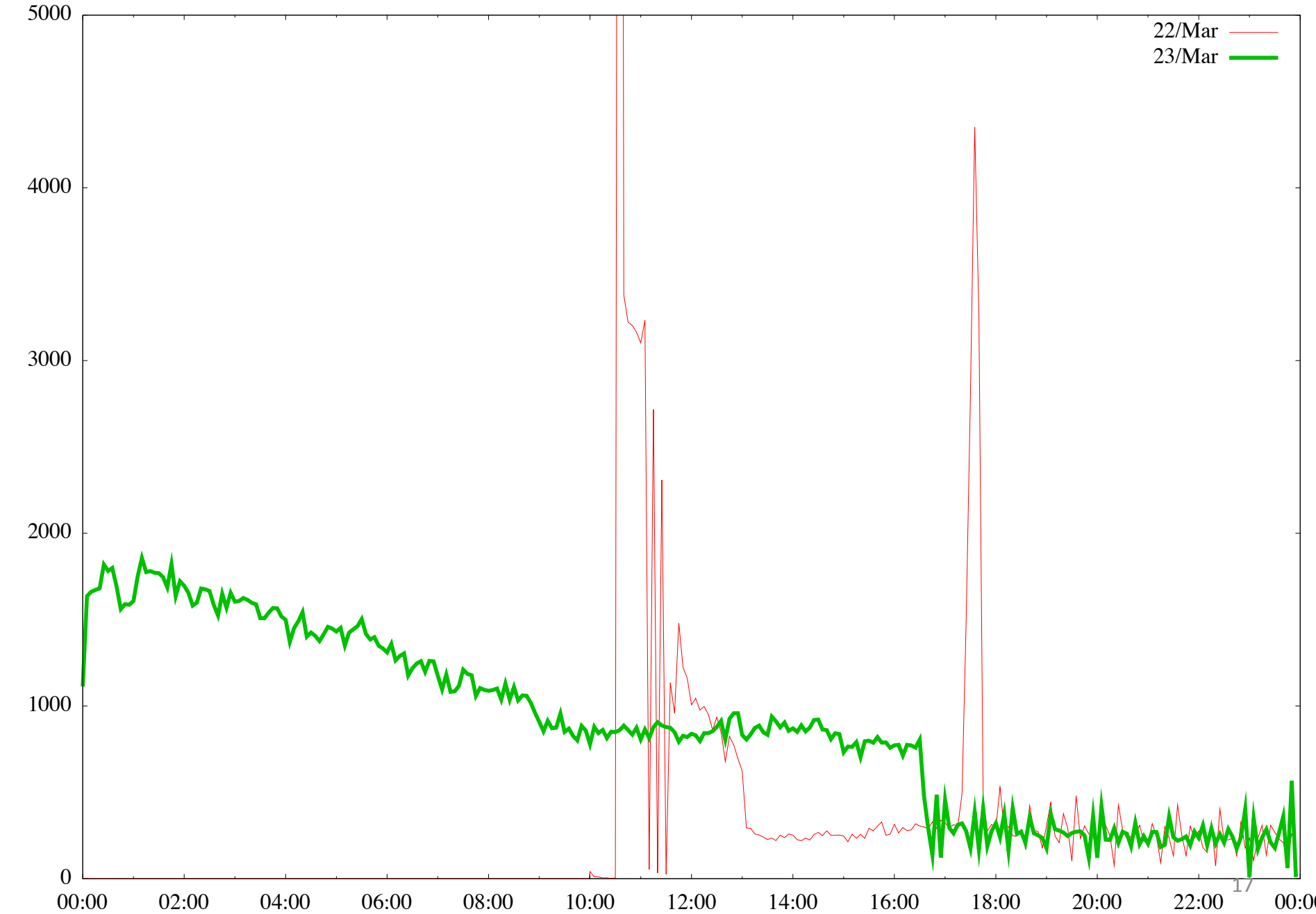
Advertising placement logic

- Budget: $100 per day, at $1.00 'CPM' max
  - Clicks per millepressions: aim to pay no more than $1 per click but pay up to $1 for a thousand impressions
- Even distribution of ads throughout the day
- No constraint on location, time
- Outcome: 350,000 placements per day, on a mostly even placement model with end of day 'soak' to achieve budget goal

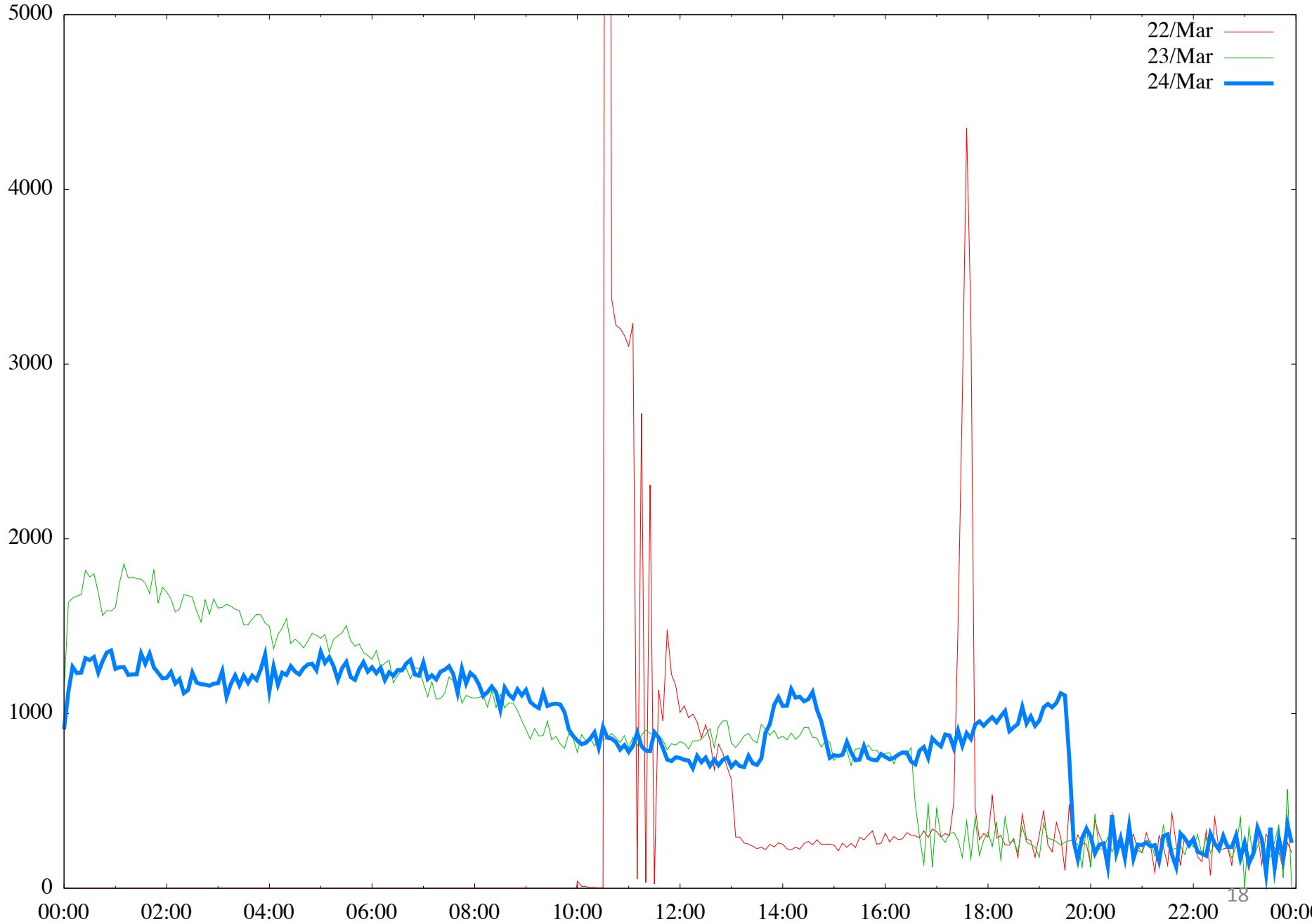
Ad Placement Training – Day 1



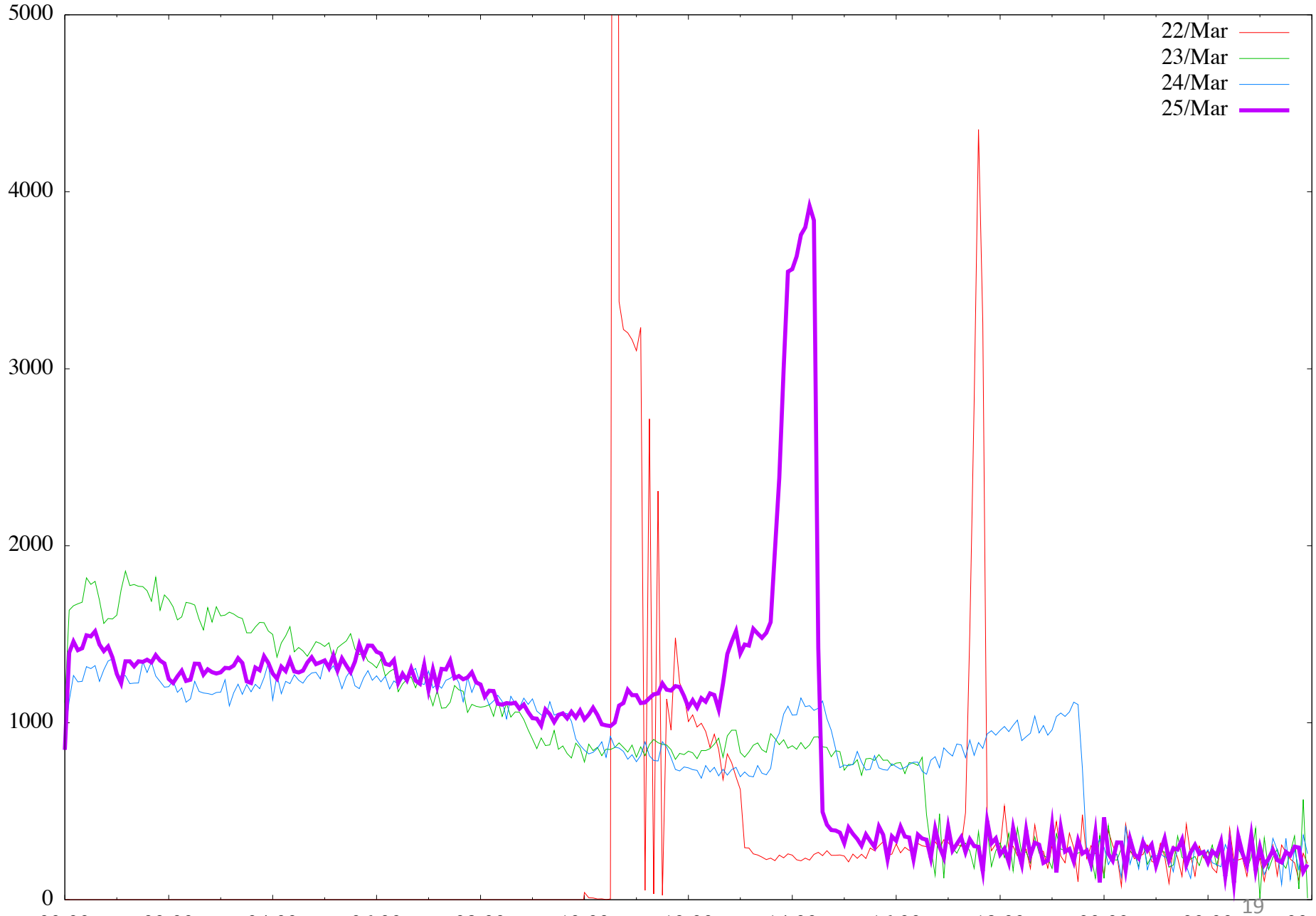
Ad Placement Training – Day 2



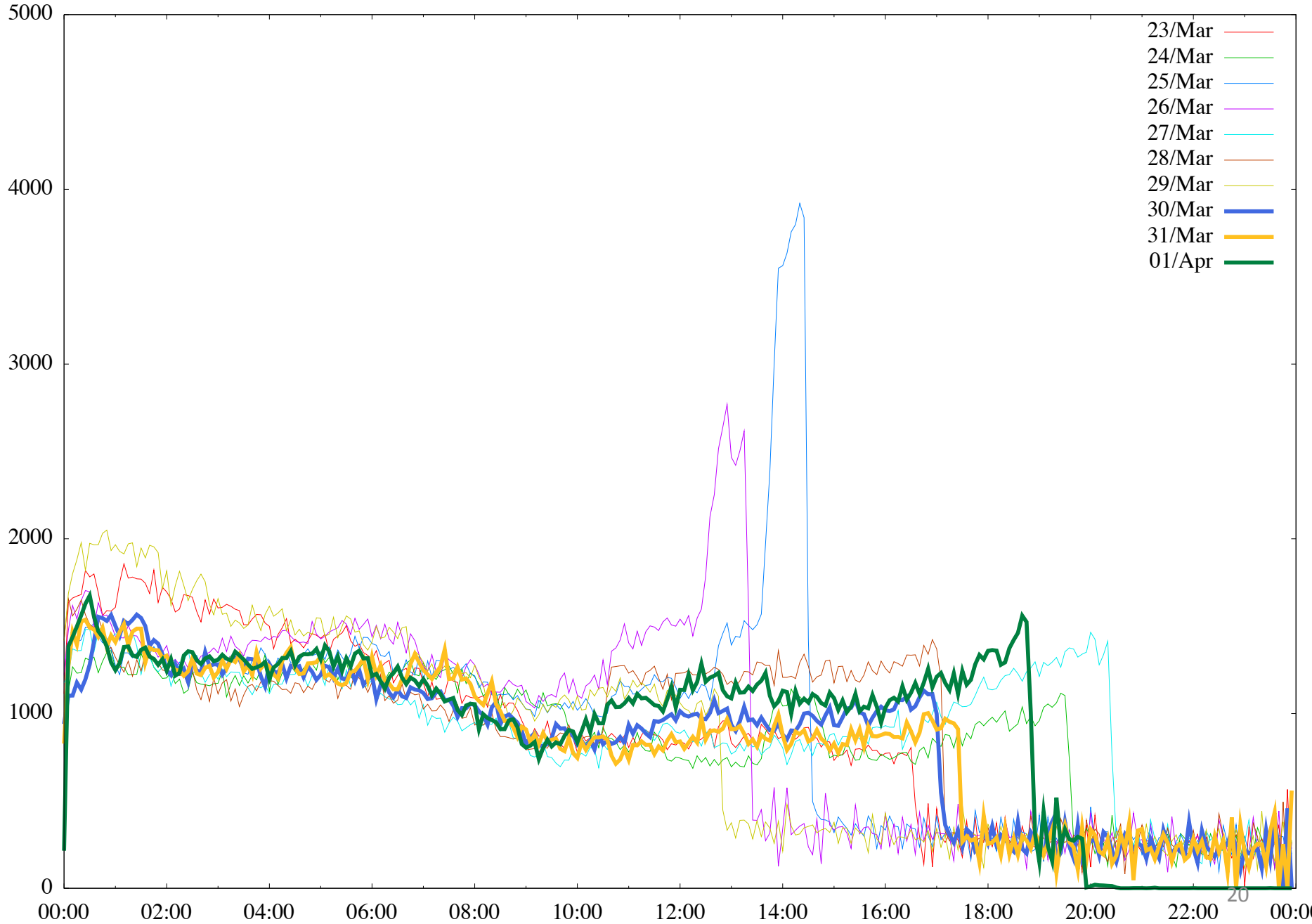
Ad Placement Training – Day 3



Ad Placement Training – Day 4



Ad Placement Training – Days 5, 6 & 7



Measurement Control Channel

- Use Flash code that is executed on ad impression that retrieves the actual measurement script
  - Ad carries code to send the client to retrieve an ad-controller URL

    http://drongo.rand.apnic.net/measureipv6id.cgi?advertID=9999
  - Client retrieves set of “tests” from the ad-controller as a sequence of URLs to fetch and a “result” URL to use to pass the results to the ad-server

- This allows us to vary the measurement experiment without necessarily altering the ad campaign itself – the ad, and its approval to run, remain unchanged so that measurements can be activated and deactivated in real time.

Experiment Server config

- There are currently three servers, identically configured (US, Europe, Australia)
- Server runs Bind, Apache and tcpdump
- Experiment directs the client to the “closest” server (to reduce rtt-related timeouts) based on simple /8 map of client address to region

Collected Data

- Per Server, Per Day:
  - http-access log

    (successfully completed fetches)
  - dns.log

    (incoming DNS queries)
  - Packet capture

    All packets

Caching

- Caching (generally) defeats the intent of the measurement
  - Although some measurements are intended to measure the effects of caching
- We use unique DNS labels and unique URL GET parameters
  - Ensures that all DNS resolution requests and HTTP fetch requests end up at the experiment's servers
- We use a common "tag" across all URLs in a single experiment
  - Allows us to join the individual fetches to create the per-user view of capability

What does this allow?

- In providing an end user with a set of URLs to retrieve we can examine:
  - Protocol behaviour

    e.g.: V4 vs V6, protocol performance, connection failure rate
  - DNS behaviours

    e.g.: DNSSEC use, DNS resolution performance…

The generic approach

- Seed a user with a set of tasks that cause identifiable traffic at an instrumented server
- The user does not contribute measurements
- The server performs the data collection

Measuring IPv6 via Ads

Client is given 5 URLs to load:

- Dual Stack object
- V4-only object
- V6-only object
- V6 literal address (no DNS needed)
- Result reporting URL (10 second timer)

All DNS is dual stack

Discovering Routing Filters via Ads

Client is given 3 URLs to load:

- DNS name that resolves into the test prefix
- DNS name the resolves to a control prefix
- Result reporting URL (10 second timer)

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)

The DNSSEC 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%	4.6%	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

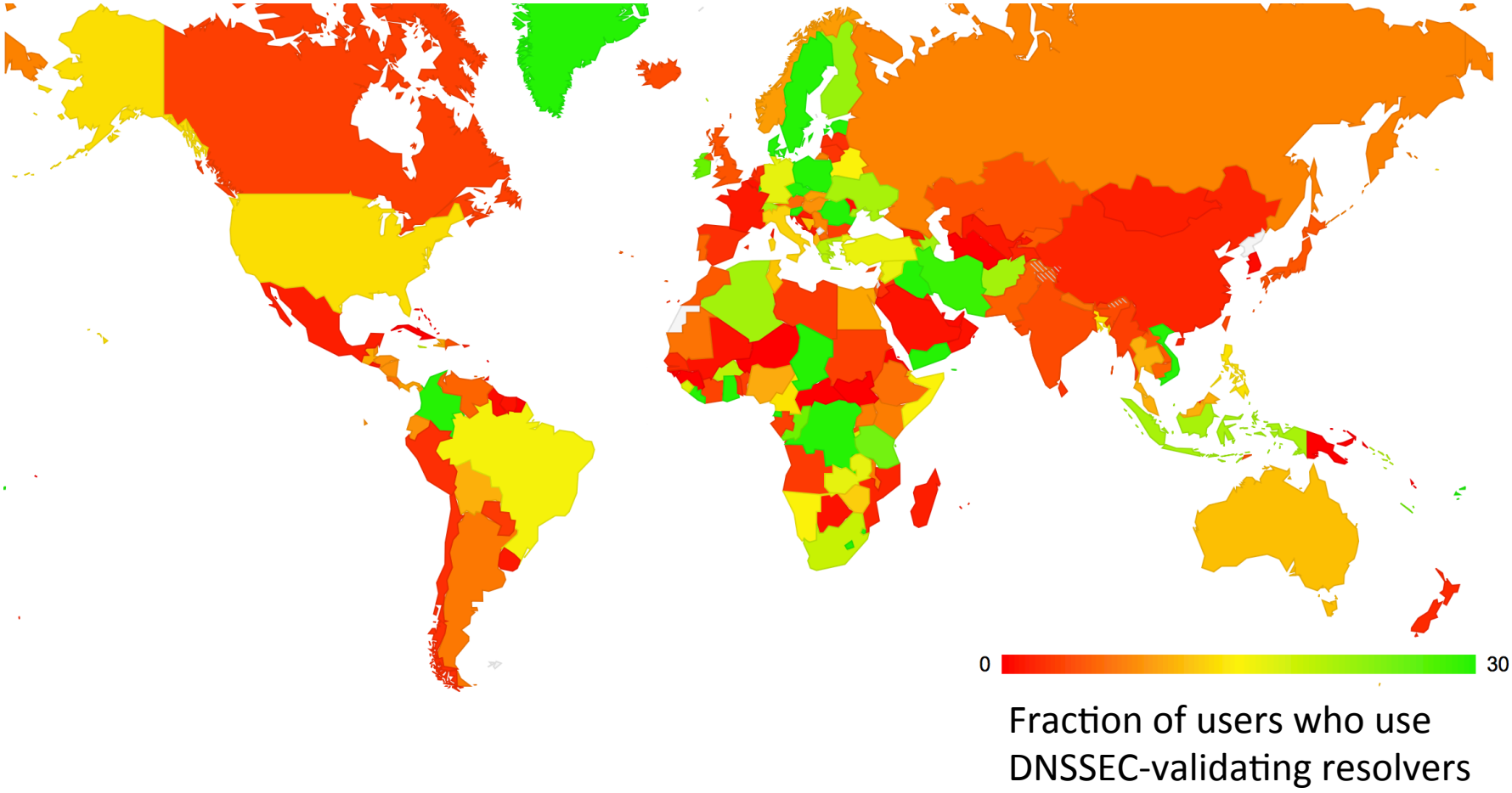
Rank	CC Code	Tests	Validating (%)	Mixed (%)	None (%)	
97	CN	1,215,241	1.9%	2.1%	96.0%	China
98	SA	45,243	1.7%	2.1%	96.2%	Saudi Arabia
99	MD	3,168	1.6%	1.9%	96.5%	Republic of Moldova
100	FR	86,888	1.6%	1.0%	97.4%	France
101	NZ	31,683	1.6%	15.0%	83.4%	New Zealand
102	BE	15,243	1.5%	3.8%	94.7%	Belgium
103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

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



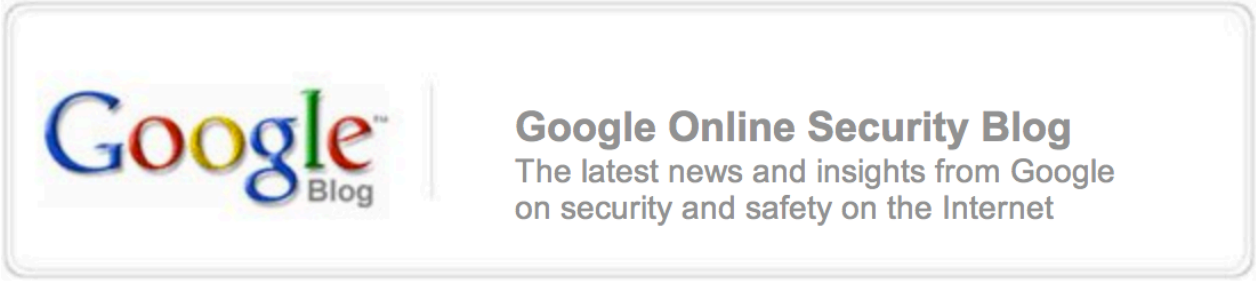
http://gronggrong.rand.apnic.net/cgi-bin/worldmap (May 2014)

Why…

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

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%	lovenia
			%	4.2%	1%	94.8%	nia
			2.4%	98.7%	1.3%	0.1%	
			1.0%	2.1%	1.8%	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**

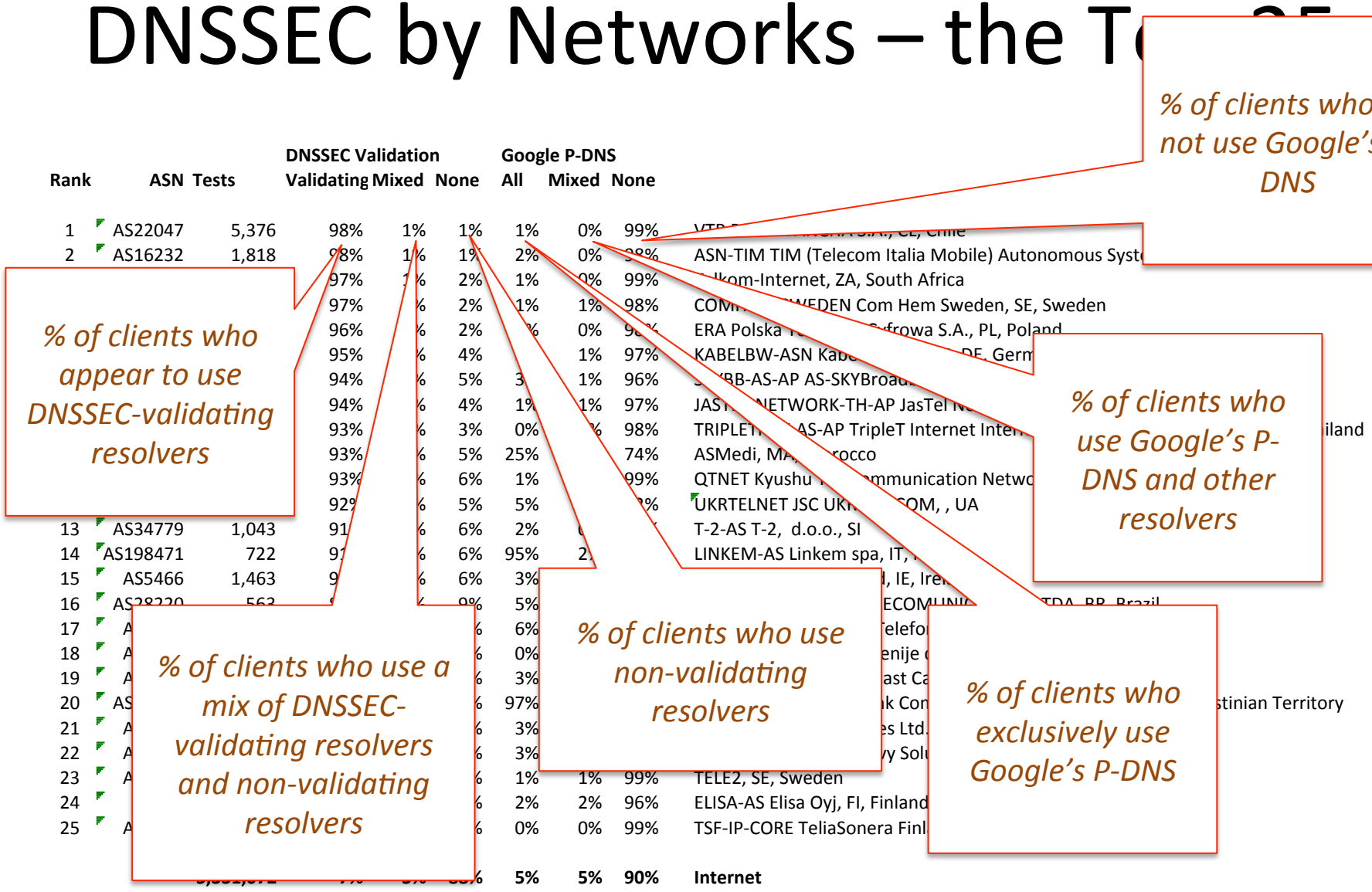
Of those clients who perform DNSSEC validation, what resolvers are they using: All Google P-DNS? Some Google P-DNS? No Google P-DNS?

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 T



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 Syst
			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%	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%		2%	UKRTELNET JSC UKR[illegible]COM, , UA
13	AS34779	1,043	91	1%	6%	2%			T-2-AS T-2, d.o.o., SI
14	AS198471	722	91	1%	6%	95%	2		LINKEM-AS Linkem spa, IT, [illegible]
15	AS5466	1,463	9	1%	6%	3%			[illegible], IE, Ire[illegible]
16	AS28220	563	[illegible]	1%	9%	5%			[illegible]ECOM UNIX[illegible]TDA, BR, Brazil
17	A[illegible]			1%	6%				Telefo[illegible]
18	A[illegible]			1%	0%				enije [illegible]
19	A[illegible]			1%	3%				ast Ca[illegible]
20	AS[illegible]			1%	97%				k Con[illegible]stinian Territory
21	A[illegible]			1%	3%				es Ltd.[illegible]
22	A[illegible]			1%	3%				y Solu[illegible]
23	A[illegible]			1%	1%	1%	1%	99%	TELE2, SE, Sweden
24				1%	2%	2%	2%	96%	ELISA-AS Elisa Oyj, FI, Finland
25	A[illegible]			1%	0%	0%	0%	99%	TSF-IP-CORE TeliaSonera Finl[illegible]
		[illegible]		1%	5%	5%	5%	90%	**Internet**

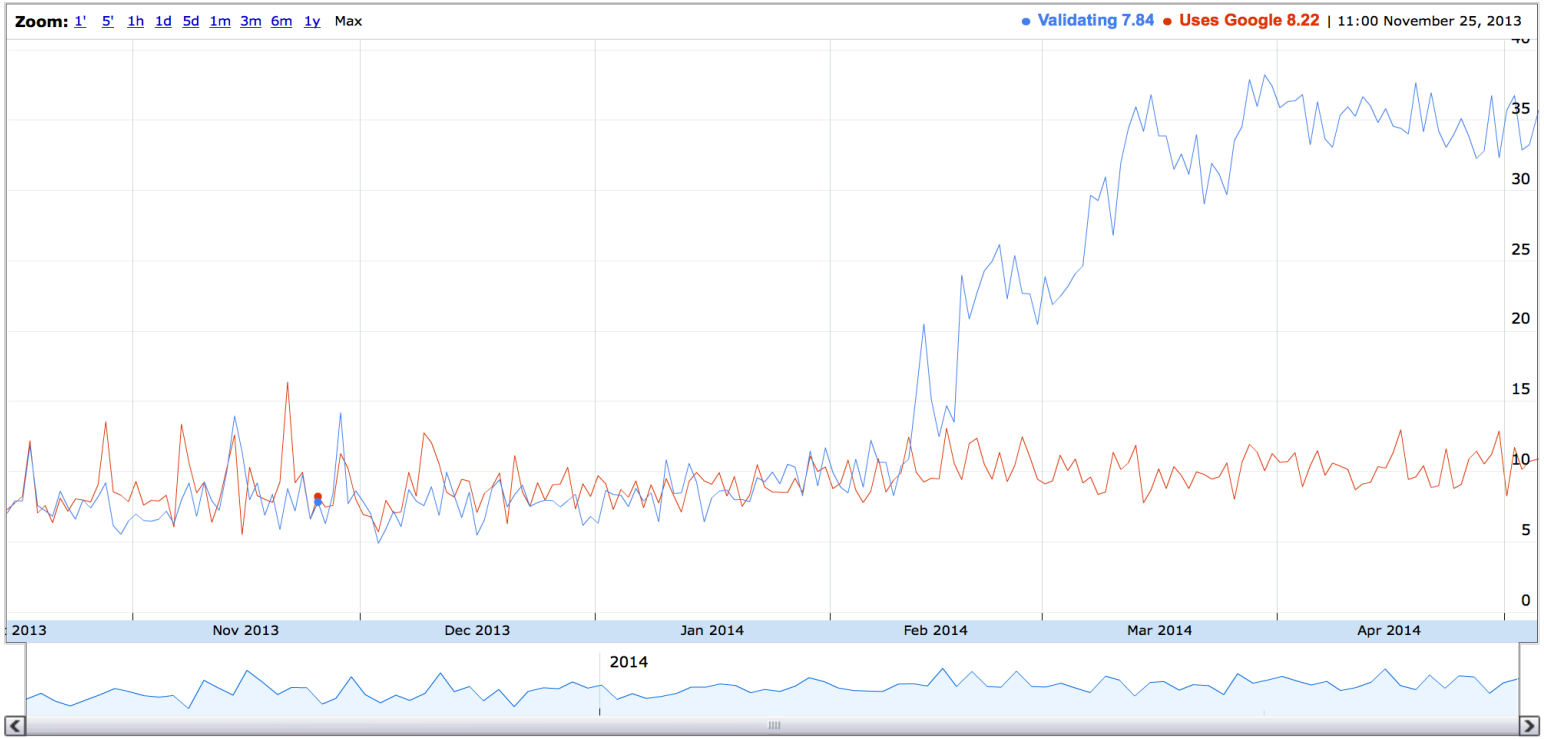
Map client IP to origin AS, and select origin ASs with more than 500 data points

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

DNSSEC Country Deployment for Poland (PL)



World Map of DNSSEC Deployment

ASN	AS Name	DNSSEC Validates	Uses Google PDNS	Samples
AS12912	TMPL T-MOBILE POLSKA SPOLKA AKCYJNA	95.62%	2.70%	3925
AS42401	ELOMZA-AS IST s.c. Malgorzata Trawinska Mariusz Trawinski	93.88%	2.04%	98
AS60624	MYNETPL-AS MyNET S.C. Tomasz Patrzalek, Marek Raton	93.24%	100.00%	74
AS35695	FALCON-AS Falcon Kalinski Bartosz	90.48%	55.56%	63
AS50121	NETMAR-AS NETMAR Mariusz Wator	89.19%	63.51%	74
AS15878	WMC-NET WMC-NET Centrum Systemow Teleinformatycznych Sp. z o.o.	89.09%	96.36%	55
AS198557	INTERMEDIA-AS PHU INTERMEDIA Przemyslaw Serweta	87.93%	100.00%	58
AS57478	DARNET-AS Dar.NET Dariusz Lyczko	87.88%	100.00%	132
AS43171	MAXNET MAXNET Lukasz Hamerski	83.61%	72.13%	61
AS42261	TECHMEDIA-AS TECH-MEDIA Michal Kaluzny	82.69%	92.31%	52
AS31628	ROBBO-AS Robbo Computer Net Robert Szamota	81.82%	97.73%	132
AS197437	PLAST-COM-AS Plast-Com	81.82%	96.97%	99

http://gronggrong.rand.apnic.net/cgi-bin/ccpage?c=PL (May 2014)

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

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

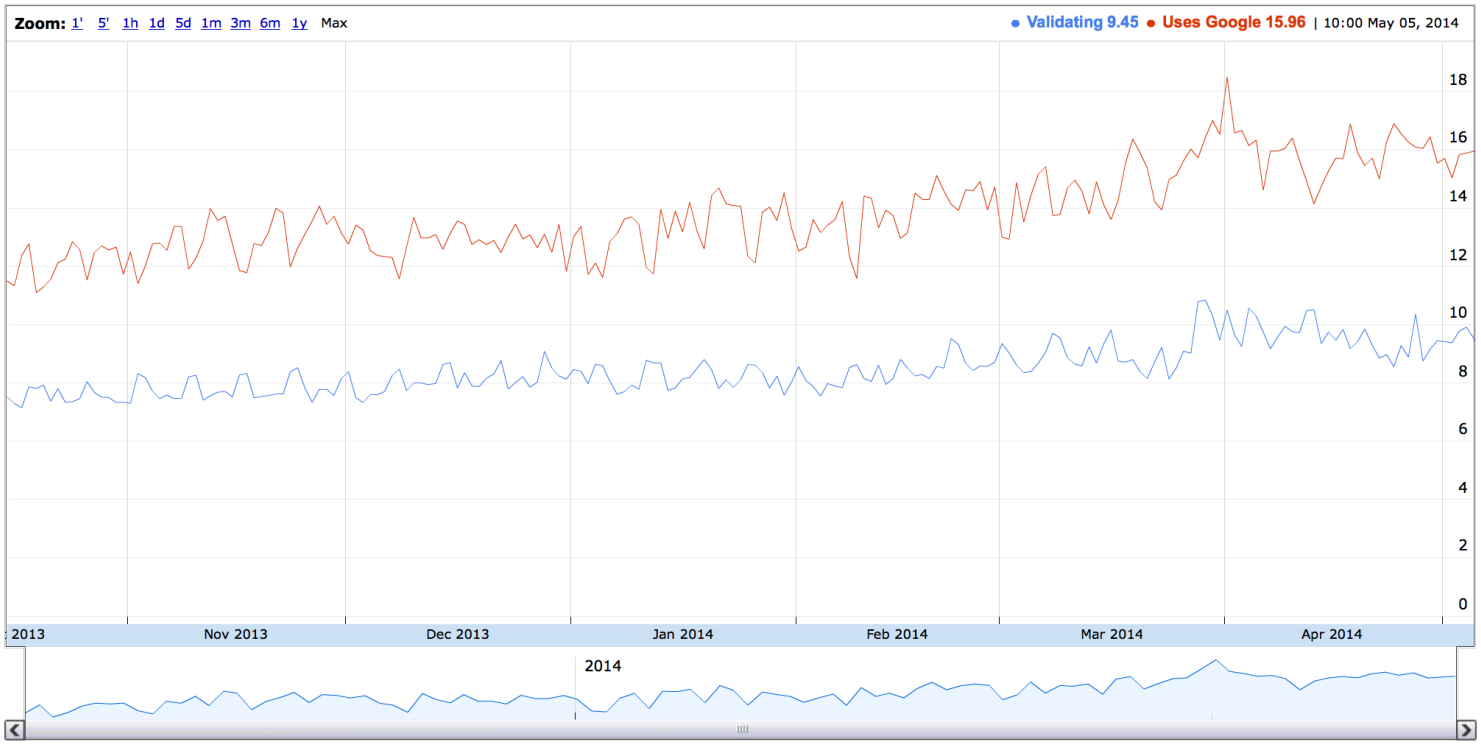
- Why do some 84% of queries have EDNS0 and the DNSSEC OK flag set, yet only 6% of clients perform DNSSEC validation?
- How come we see relatively more queries with the DNSSEC OK flag set for queries to domains in signed zones?

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
  - 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

DNSSEC Country Deployment for World (XA)

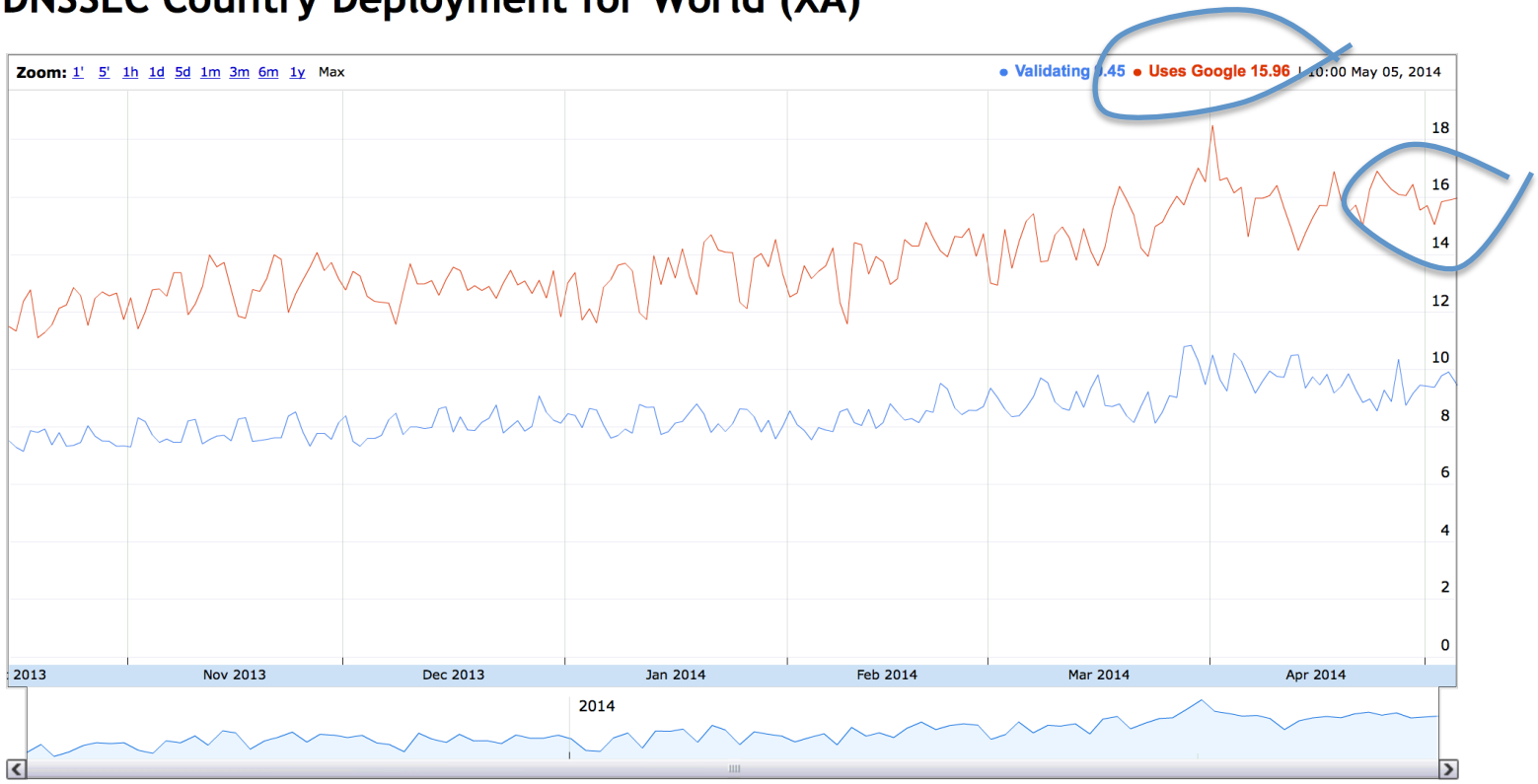


World Map of DNSSEC Deployment

Code	Region	DNSSEC Validates	Uses Google PDNS	Samples
XA	World	9.22%	15.21%	63021492
XC	Americas	12.44%	13.96%	16819056
XE	Europe	12.14%	7.84%	13327956
XF	Oceania	11.10%	5.06%	567483
XB	Africa	10.15%	24.81%	2937888
XD	Asia	6.24%	17.71%	29369103
XG	Unclassified	0.00%	100.00%	11374

Some things to think about

DNSSEC Country Deployment for World (XA)



World Map of DNSSEC Deployment

Code	Region	DNSSEC Validates	Uses Google PDNS	Samples
XA	World	9.22%	15.21%	63021492
XC	Americas	12.44%	13.96%	16819056
XE	Europe	12.14%	7.84%	13327956
XF	Oceania	11.10%	5.06%	567483
XB	Africa	10.15%	24.81%	2937888
XD	Asia	6.24%	17.71%	29369103
XG	Unclassified	0.00%	100.00%	11374

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/"
```

A few observations

- Measuring what happens at the user level by measuring some artifact or behaviour in the infrastructure and inferring some form of user behaviour is going to be a guess of some form
- If you really want to measure user behaviour then its useful to trigger the user to behave in the way you want to study or measure
- The technique of embedding code behind ads is one way of achieving this objective, for certain kinds of behaviours relating to the DNS and to URL fetching

Questions?

APNIC Labs:

Geoff Huston research@apnic.net