July 2013
Geoff Huston

DNS, DNSSEC and Google's Public DNS Service

For some time now we've been tracking the progress of the deployment of DNSSEC in the Internet. Its been a story of an evolution of the measurement technique, starting with a technique that attempted to guess at the behaviour of resolvers (http://www.potaroo.net/ispcol/2012-10/counting-dnssec.html), through to techniques that explicitly pose novel DNS names to clients so as to negate aspects of resolver caching that otherwise complicate the measurement technique (http://www.potaroo.net/ispcol/2013-04/dnssec-google.html).

In the process we've learned perhaps more than we had wanted to about the behaviour of Flash engines, Apache web servers and FreeBSD system tuning, and also learned much more than we had anticipated about the finer details of Google's online ad presentation behaviour. But one thing we did not see in all of this was any large scale jumps in the level of client use of DNSSEC validation over this period at the start of the year.

This apparent slowness in the adoption of DNSSEC a source of some frustration. We have heard many times that some of the more insidious threats to the security and integrity of the Internet's service environment start with attacks on the DNS. Such attacks exploit a real weakness in the behaviour of many users: You type in a URL, and you see a familiar screen in response and you think you are now connected to the service you specified. But there is the risk that you are not, and this risk is there irrespective of whether the service is "secure" or not. There is a risk from various forms of so-called "man-in-the-middle" attacks that you have been mislead. Most such attacks pass largely unremarked, if not unnoticed. But from time to time the issue generates a high level of public prominence, such as the attacks that resulted from Diginotar attack on a Domain Name Certification Authority back in 2011 and the subsequent exploitation of that attack in a consequent structured attack on Gmail users located in Iran (http://www.potaroo.net/ispcol/2011-10/hacking.html).

The best defence against these forms of attack that we've been able to devise is to secure the DNS, so that a system making a query of the DNS can be assured that the answer that they are given in response to their query is precisely the same information that was entered into the DNS by the authorized zone administrator. This, in turn, allows the embedding of information about domain name certification into the DNS in a secure manner (as described in RFC6394), which is a relatively effective response to the form of man-in-the-middle attack we saw as a consequence of the compromise of Diginotar's CA services. The combination of these two measures, signing the domain name using DNSSEC, and placing certificate credentials into the DNS as signed data, would allow a user's browser to reliably avoid using a compromised CA to validate a fake Domain Name Certificate.

For some years attention has been focussed to the effort to deploy DNSSEC in the domain name system. We have seen an extensive effort to get to a DNSSEC-signed root, and now that this has been achieved, we are now seeing this effort focus on the signing of all top level domain names (TLDs).

But signing domain names is only one half of the story. Clients' DNS resolvers also need to retrieve this information and validate the responses they receive from the DNS. So, at the other end of the spectrum, in the realm of DNS resolvers, we have seen increasing use of DNSSEC validation, but little in the way of structured measurement of progress in this area. At APNIC Labs have been looking at

ways to measure this, and are trying to answer the basic question: *How many of the Internet's user population exclusively use DNS resolvers that perform DNSSEC validation?*

In late 2012 we saw some 1.6% of clients exclusively use DNSSEC-validating resolvers, using a relatively imprecise measurement methodology (http://www.potaroo.net/ispcol/2012-10/counting-dnssec-2.html).

At the start of 2013 we revised the experimental technique, and saw some 3% of users appear to exclusively use DNSSEC validating resolvers. Appropriately, these users were unable to resolve a DNS name when its DNSSEC signature was invalid. In the same experiment, we also measured a further 2% of clients who use a mix of DNSSEC-validating and non-validating resolvers, so that when a DNSSEC validating resolver correctly responds with SERVFAIL the client then queries another resolver who does not perform DNSSEC validation, and therefore dutifully returns the original address record (http://www.potaroo.net/ispcol/2013-04/dnssec-google.html).

A couple of weeks after we conducted this experiment Google announced the inclusion of DNSSEC validation to its public DNS service (http://www.theregister.co.uk/2013/03/20/google_adds_dnssec_validation/). Earlier configurations of Google's public DNS service required the client to set the DNSSEC OK (DO) flags on its queries in order to trigger a DNSSEC validation operation, but in late March Google switched this behaviour to perform a DNSSEC validation for all queries, except for those that explicitly requested no validation via the setting of the Checking Disabled (CD) flag in the DNS query.

What did we see in May when we again measured DNSSEC use by the Internet's end user population?

Measuring DNSSEC Use

We ran an experiment across the period of the 9th May through to the 26th May, and ran a DNSSEC capability test across 2,746,777 clients, selected using an online advertisement placement method. Of these clients we saw 2,595,672 complete the experiment's tests and submit results to our server.

As with previous DNSSEC experiments, we presented the client with three URLs, all using IPv4. URL A used a domain name that was validly DNSSEC-signed domain name. URL B had no DNSSEC signature. URL C had a DNSSEC signature that was corrupted so that DNSSEC validation would fail. All three URLs used a label part in their DNS name that was relatively. Through this measure we were trying the minimize any measurement "noise" as a result of DNS caching, ensuring that all queries were passed to the authoritative name server for both queries for the original resource records and queries for the DNSSEC DS and DNSKEY resource.

> To explain "relative uniqueness" a little more, we wanted to present each client with a unique DNSSEC signed domain name. The most obvious way to achieve this would be to use a large signed zone, but there are a number of major operational considerations in maintaining a signed DNS zone file with upward of 10 million entries that would be needed to support an experiment of this scale. Instead, we opted to use a smaller pool of some 500,000 unique names, and set a one hour TTL on the DNS data. We were cycling through this name space in around 20 hours, which was considered to be comfortably in excess of the one hour TTL.

The various combination of URLs that were logged as being fetched from the associated web server produced the outcomes as shown in Table 1. This table also includes results from the earlier run of this experiment in February of this year.

	URL A	URL B	URL C	Count	%	% (Feb'13)
1	no	no	no	3,040	0.1%	0.6%
2	yes	no	no	1,348	0.1%	0.1%
3	no	yes	no	4,445	0.2%	0.1%
4	**yes**	**yes**	**no**	**216,700**	**8.3%**	**3.5%**
5	no	no	yes	1,275	0.1%	0.1%
6	yes	no	yes	4,388	0.2%	0.1%
7	no	yes	yes	5,044	0.2%	0.2%
8	**yes**	**yes**	**yes**	**2,359,462**	**90.9%**	**95.3%**

Table 1 – DNSSEC Fetch Results (Web)

If a client supports DNSSEC validation outcomes then it would fetch URLs A and B, but not URL C (row 4 in Table 1). If it does not support DNSSEC validation then it should fetch all three URLs, as in all other respects the three URLs are functionally identical (row 8 in Table 1). However, some 3% of clients fetch various combinations of URLs other than these two anticipated combinations, showing that there is some variability in the precise mode of execution of the experiment in certain client scenarios.

The web server logs of this experiment show that, within an error bound of ±1%, some **8%** of clients appear to be performing some kind of DNSSEC validation, based on the combinations of URLs that they are able to fetch. This represents an increase of some 5% since February, which we could surmise as being attributable to the change in behavior of the Google Public DNS resolvers.

A detailed examination of the logs of the DNS authoritative server, when coupled with the Web log data can provide a better insight into these numbers. We are looking for clients whose DNS resolvers query for both the A resource record and the DNSKEY and DS resource records, and where the client fetches the A and B URLs, but not the C URL. These clients, we assume, are using DNS resolvers that perform DNSSEC validation, and pass the client a SERVFAIL response to the DNS query associated with the C URL. Furthermore, we can assume that where a client's DNS resolvers make no query for URL A or C's DS or DNSKEY resource records, then we can assume that the client's DNS resolvers perform no DNSSEC. The other case is where we see the retrieval of DNSSEC resource records, but see fetching of the C URL. We assume that in this case the client's DNS resolvers are a mix of validating and non-validating resolvers, and in the case of the C URL the response of SERVFAIL from a DNSSEC-validating resolver causes the client to ask the same query from the next resolver in its local resolver set, or causes its DNS resolver to ask the next resolver in its DNS forwarding set without the client's explicit knowledge.

We can combine both the DNS query profile and the web server logs to produce the results shown in Table 2.

Client Behaviour	Count	%	% (Feb'13)
DNSSEC Validating	**209,505**	**8.1%**	**3.3%**
Mix of Resolvers	110,701	4.4%	2.6%
NO DNSSEC	2,206,592	87.3%	94.1%

Table 2 – DNSSEC Fetch Results (DNS)

This DNS data shows that the proportion of clients who exclusively use DNS resolvers that perform DNSSEC validation has risen by a little under 5% of the total client population, from 3.1% in February 2013 to **8.3%** in May 2013.

We have also seen a significant rise in the number of clients who use a mix of DNS resolvers, some of which were seen to perform DNSSEC validation. This has risen by some 1.8%, from 2.6% in February 2013 to 4.4% in May 2013.

To what extent is this increase in the population attributable to Google's Public DNS servers?

Of the 2.34M unique IP addresses of clients who ran this experiment, we saw 174,082 clients use Google Public DNS servers, or 7.4% of all tested clients. Of these, we saw some 128,359, or 5.5% of all clients exclusively use Google's Public DNS servers, with the remaining 45,723 (or 2%) clients use a mix of Google DNS servers and other servers.

More specifically, where are these DNSSEC-validating clients, and what resolvers do they use?

Of those countries with more than 200 samples, those countries with the highest proportion of DNSSEC-validating clients are as follows:

Rank	CC	Count	%DNSSEC	%Mixed	%No DNSSEC	Country
1	SE	7,082	79.64	4.90	15.46	Sweden
2	SI	5,357	60.35	6.03	33.62	Slovenia
3	AG	313	57.51	8.63	33.87	Antigua and Barbuda
4	LU	734	46.59	7.08	46.32	Luxembourg
5	AO	247	42.91	21.46	35.63	Angola
6	FI	2,748	39.30	16.78	43.92	Finland
7	VN	30,273	38.41	4.06	57.53	Vietnam
8	CZ	33,005	34.97	8.27	56.76	Czech Republic
9	CL	52,924	31.22	8.45	60.33	Chile
10	JM	1,752	30.02	3.20	66.78	Jamaica
11	IE	8,985	28.79	5.49	65.72	Ireland
12	NC	290	27.93	5.52	66.55	New Caledonia
13	BB	1,476	25.81	1.69	72.49	Barbados
14	FO	242	24.79	0.83	74.38	Faroe Islands
15	UA	27,934	23.17	12.70	64.13	Ukraine
16	ID	63,288	22.84	8.06	69.10	Indonesia
17	ZA	3,333	22.47	9.72	67.81	South Africa
18	US	165,630	19.91	3.59	76.50	United States of America
19	TR	52,909	19.39	2.22	78.39	Turkey
20	AF	232	18.53	34.05	47.41	Afghanistan
		2,871,753	**8.73**	**6.93**	**84.34**	**World**

Table 3 – DNSSEC Validation by Country

There are not many country tables where the Faroe Islands features in the top 20, but of the 242 tests we ran against clients located in the Faroe Islands we found one quarter of them performed a full DNSSEC validation.

A complete list of all countries and their counts of clients who perform DNSSEC validation can be found at http://www.potaroo.net:/ispcol/2013-07/may_by_country.csv.

To what extent can these results be attributed to Google's Public DNS service? Table 4 shows the same 20 countries, but with additional columns added, namely the proportion of use of Google's Public DNS service, and also looking at just the subset of end clients who are observed to perform DNSSEC validation, and the proportion of these clients who use Google's Public DNS Service.

Rank	CC	Count	DNSSEC (%)			Google Public DNS (%)			DNSSEC + Google DNS (%)				Country
			Valid	Mixed	Not	All	Mixed	None	Count	All	Mixed	None	
1	SE	7,082	**79.64**	4.90	15.46	2.27	1.28	96.44	5640	1.84	0.23	97.93	Sweden
2	SI	5,357	**60.35**	6.03	33.62	5.30	0.62	94.08	3233	7.42	0.28	92.30	Slovenia
3	AG	313	**57.51**	8.63	33.87	4.47	2.56	92.97	180	4.44	0.56	95.00	Antigua and Barbuda
4	LU	734	**46.59**	7.08	46.32	1.77	0.14	98.09	342	1.75	0.00	98.25	Luxembourg
5	AO	247	**42.91**	21.46	35.63	18.22	6.88	74.90	106	1.89	7.55	90.57	Angola
6	FI	2,748	**39.30**	16.78	43.92	1.31	0.29	98.40	1080	2.31	0.28	97.41	Finland
7	VN	30,273	**38.41**	4.06	57.53	39.23	2.93	57.84	11629	96.60	2.30	1.10	Vietnam
8	CZ	33,005	**34.97**	8.27	56.76	7.02	2.82	90.15	11543	11.87	3.99	84.15	Czech Republic
9	CL	52,924	**31.22**	8.45	60.33	1.57	1.00	97.43	16524	3.55	0.42	96.03	Chile
10	JM	1,752	**30.02**	3.20	66.78	28.65	0.63	70.72	526	91.83	0.57	7.60	Jamaica
11	IE	8,985	**28.79**	5.49	65.72	4.26	1.69	94.05	2587	11.94	1.01	87.05	Ireland
12	NC	290	**27.93**	5.52	66.55	4.14	1.72	94.14	81	11.11	0.00	88.89	New Caledonia
13	BB	1,476	**25.81**	1.69	72.49	2.71	0.14	97.15	381	8.14	0.26	91.60	Barbados
14	FO	242	**24.79**	0.83	74.38	1.65	0.00	98.35	60	3.33	0.00	96.67	Faroe Islands
15	UA	27,934	**23.17**	12.70	64.13	12.03	3.15	84.82	6473	20.22	2.39	77.38	Ukraine
16	ID	63,288	**22.84**	8.06	69.10	17.60	5.75	76.65	14454	68.19	12.85	18.96	Indonesia
17	ZA	3,333	**22.47**	9.72	67.81	3.75	2.16	94.09	749	6.68	1.87	91.46	South Africa
18	US	165,630	**19.91**	3.59	76.50	3.16	1.10	95.75	32985	7.27	0.75	91.98	United States of America
19	TR	52,909	**19.39**	2.22	78.39	19.55	1.71	78.74	10260	93.36	3.25	3.39	Turkey
20	AF	232	**18.53**	34.05	47.41	24.57	27.59	47.84	43	72.09	13.95	13.95	Afghanistan
		2,871,753	**8.73**	6.93	84.34	5.63	3.73	90.64	250635	46.63	6.25	47.12	World

Table 4 – DNSSEC Validation and use of Google's Public DNS by Country

The relative number of clients who exclusively use Google's Public DNS service is prominent in Vietnam, Jamaica and Afghanistan, while the relative number of clients who use Google's DNS service in conjunction with other servers is prominent in Angola, Indonesia and Turkey.

If we look at the subset of clients who are seen to be performing DNSSEC validation, then there is a very strong correlation between the use of Google's Public DNS resolvers and DNSSEC validation in Vietnam, Jamaica and Indonesia. In other countries in this list it would appear that there are other resolvers used by these clients that also are performing DNSSEC validation.

What we find for the entire data set gathered in May 2013, is that of the 240,635 end clients who are performing DNSSEC validation, some 47% of these clients use Google's Public DNS service exclusively, another 47% of these clients do not appear to use Google's Public DNS service, and the remaining 6% use a mix of Google's and other DNS resolvers.

What this shows is that some 4% of the Internet's user base exclusively use Google's Public DNS service and now are having their DNS names validated by this public DNS service. A further 4% of users also use DNS resolvers that perform DNSSEC validation, but do not use Google's public DNS service to do so.

But doesn't the final line of table 4 indicate that 5.6% of the tested clients exclusively use Google's Public DNS? Does this mean that 1.6%, or 45,000 clients, who are exclusively using Google's Public DNS are not performing DNSSEC validation? It would appear so. Part of the issue with measuring DNS is that an authoritative server cannot unravel the manner by which a DNS query is passed from a client through a DNS forwarder chain before it reaches an authoritative name server. If a DNS Forwarder passes all its queries to Google's Public DNS service, but marks all its queries with DNSSEC Checking Disabled, then we would see queries from Google's public DNS resolvers that are not apparently performing DNSSEC validation. This would appear to be the case here, and this is the most likely explanation for these "missing" 45,000 DNSSEC validating clients.

Table 4 displayed a country-by-country view of DNSSEC deployment. What is the view of DNSSEC use when looking at service provider networks? This is shown in Table 5.

Rank	ASN	Count	DNSSEC (%)			Google Public DNS (%)			DNSSEC + Google DNS (%)				AS Name
			Valid	Mixed	Not	All	Mixed	None	Count	All	Mixed	None	
1	34630	208	98.08	0.96	0.96	98.08	0.96	0.96	204	99.02	0.98	0.00	AMBRA RO
2	44034	351	97.72	1.14	1.14	1.99	0.28	97.72	343	2.04	0.00	97.96	HI3G Hi3G Access SE
3	197121	478	97.28	0.84	1.88	0.63	0.21	99.16	465	0.65	0.22	99.14	DIODOS Research Net GR
4	12912	1632	97.12	1.78	1.10	2.33	0.12	97.55	1585	2.27	0.13	97.60	Polska Telefonia PL
5	27831	713	96.91	2.95	0.14	1.40	0.42	98.18	691	0.43	0.00	99.57	Colombia Mobil CO
6	44143	408	96.81	2.21	0.98	0.00	0.98	99.02	395	0.00	1.01	98.99	Vip mobile RS
7	5628	530	96.79	1.89	1.32	2.45	0.38	97.17	513	1.56	0.39	98.05	Slovak Telecom SK
8	198471	762	96.59	1.18	2.23	97.38	0.66	1.97	736	99.73	0.27	0.00	Linkem spa IT
9	39651	971	96.50	2.47	1.03	0.82	0.00	99.18	937	0.85	0.00	99.15	Com Hem Sweden SE
10	34779	976	96.41	1.33	2.25	1.43	0.41	98.16	941	1.38	0.32	98.30	T-2 SI
11	34525	299	96.32	1.67	2.01	0.00	0.33	99.67	288	0.00	0.35	99.65	KoBa Konrad Baranowski PL
12	44489	482	96.27	1.66	2.07	2.90	1.87	95.23	464	2.37	1.94	95.69	STARNET Starnet CZ
13	52400	315	96.19	1.27	2.54	96.83	0.63	2.54	303	99.67	0.33	0.00	Olo del Peru PE
14	5603	1564	96.10	1.53	2.37	0.64	0.19	99.17	1503	0.60	0.20	99.20	Telekom Slovenije SI
15	27668	525	95.81	2.48	1.71	7.43	0.76	91.81	503	7.36	0.60	92.05	ETAPA EP EC
16	37457	499	94.59	2.20	3.21	1.20	0.20	98.60	472	1.27	0.21	98.52	Telkom-Internet ZA
17	719	706	94.33	2.97	2.69	0.99	0.42	98.58	666	1.05	0.15	98.80	ELISA-AS Elisa Oyj EU
18	29562	852	94.01	3.99	2.00	1.17	0.00	98.83	801	1.12	0.00	98.88	Kabel BW GmbH DE
19	39309	213	92.02	2.82	5.16	1.41	1.41	97.18	196	1.02	1.53	97.45	EDUTEL-AS Edutel B.V. NL
20	6849	5184	91.94	3.09	4.98	3.97	1.99	94.04	4766	3.42	1.68	94.90	UKRTELECOM UA

Table 5 – DNSSEC Validation and use of Google's Public DNS by Origin AS

Table 5 shows a similar analysis of the DNSSEC data, but this time using the originating network, or Autonomous System, rather than country. Of the top 20 DNSSEC validating networks with more than 200 users seen in this experiment, only three networks, Ambra (AS 34630) in Romania, Linkem (AS 198471) in Italy, and Olo Peru (AS 52400) in Peru, appear to have directed all their customers' DNS queries to Google's DNS systems. The other 17 networks in this list all appear to be using local DNS resolvers that have been configured to perform DNSSEC validation.

A full list of all networks, and their counts of clients who perform DNSSEC validation, can be found at http://www.potaroo.net:/ispcol/2013-07/may_by_originas.csv.

Google's Public DNS Service

Since March 2013 we've seen the proportion of end users who use DNSSEC resolvers that perform DNSSEC validation rise from 3.3% to 8.1%, or a rise of some 4.7%.

Most, but not all of this rise, can be attributed to Google's Public DNS service, which is used exclusively by some 5.6% of all clients across the entire Internet. When Google turned on DNSSEC validation on their resolvers then the majority of these clients were then performing DNSSEC validation even though they had not changed any part of their local DNS configuration. Just over one half of all clients who are seen to be performing DNSSEC validation, use Google's Public DNS Servers.

However, that's not the total population of users who avail themselves of Google's DNS services. A further 3.7% of users also use Google's Public DNS service, but they use it in conjunction with other DNS resolvers. The most common case here is that the other DNS resolvers used by the client, or by the client's local DNS resolver, do not use DNSSEC validation, so the SERVFAIL response from the query to Google's service prompts additional DNS queries to be made to other configured DNS resolvers. A total of 9.4% of the clients we saw in this experiment made use of Google's Public DNS service in one way or another.

Performing DNS resolution for almost 10% of the Internet is a very significant undertaking by Google. There are some interesting issues that this figure raises in terms of the breadth and volume of information about user behaviors that is exposed in DNS queries. In the light of the current concerns

over the use of so-called Internet meta-data by a number of national intelligence operations, and broader concerns relating to individual privacy and the use of various forms of cloud services and other public services, this aspect of today's DNS operations raises some further questions about extent to which certain aspects of user behaviors are visible to this individual DNS operator though the use of their DNS systems by some 10% of the Internet's user population. However, that is perhaps heading down the path of a new topic, and is straying from this study of the level of deployment of DNSSEC validation in today's DNS.

On the topic of DNSSEC deployment, we'll continue to track the state of DNSSEC deployment in the coming months, to see how and where the story of DNSSEC deployment evolves.

Disclaimer

About the Author

Geoff Huston B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region. He has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for the initial build of the Internet within the Australian academic and research sector. He is author of a number of Internet-related books, and was a member of the Internet Architecture Board from 1999 until 2005, and served on the Board of Trustees of the Internet Society from 1992 until 2001.

www.potaroo.net