The ISP Column
A monthly column on things Internet

October 2012

Geoff Huston,
George Michaelson

Re-counting DNSSEC

This is a followup article to *Counting DNSSEC* that reflects some further examination of the collected data. This time I'd like to describe some additional thoughts about the experiment, and some revised results in our efforts to count just how much DNSSEC is being used out there.

And for those looking for just the answers, here's a quick summary of the recount. It appears that as of September 2012 when this experiment was performed some 1.7% of the visible DNS resolvers in the Internet are performing DNSSEC validation, and some 1.6% of all end client systems are exclusively using DNSSEC validating resolvers.

And now the details…

The Experiment

Firstly, I should briefly recap on the experiment itself. We used an online advertisement delivery system as a means of enrolling end user systems to perform a simple DNSSEC capability experiment. Many online advertisement systems support dynamic content, and in this Adobe Flash was used with the code configured to perform the necessary dynamic support for the measurement exercise. We configured the ad to generate two unique URLs for the user's browser to fetch. The URLs are of the form:

```
http://t10000.u5951826831.s1347594696.i767.v6022.d.t5.dotnxdomain.net/1x1.png
http://t10000.u5951826831.s1347594696.i767.v6022.e.t6.dotnxdomain.net/1x1.png
```

The 's' and 'u' fields are dynamically generated, and the combination is unique for each user that is presented with an impression of the ad. This means that every client will generate a query for resolution of a unique DNS name, so that any caching of the outcome of the DNS query for one instance of this experiment will not be used by any other instance of this experiment, even if the users share the same DNS resolver. This form of dynamic DNS label generation also eliminates any URL object caching.

In this experiment we have used two subdomains, both of which are DNSSEC signed, and each zone consists of a single wildcard. The only difference between the two subdomains lies in the DNSSEC configuration. In the case of one subdomain (`t5.dotnxdomain.net`) the DS records are correctly configured in the `dotnxdomain.net` zone, while in the case of the other subdomain (`t6.dotnxdomain.net`) the DS records are deliberately altered. The intended consequence is that DNSSEC validation of domain names in `t5.dotnxdomain.net` will succeed, while DNSSEC validation in the other subdomain, `t6.dotnxdomain.net`, will fail.

The experiment script includes a 10 second timer. At the expiration of this timer the client will perform a GET where the parameters to the GET record the locally measured status of the fetches of the above two URLs. This result GET is directed to a URL whose DNS name part is not DNSSEC-signed.

DNSSEC use from the Logs

The experiment was in operation for 17 days, from the 10th of September 2012 until the 27th of September 2012:

Advertisement Placement Report:	4,965,129
DNS Query Log: Unique Identifiers:	3,816,822
Web Query Logs: Unique Identifiers:	2,831,780

The difference between the advertisement placement report and the DNS query log indicates that some 23% of the ads were aborted before the control script had a chance to execute the first DNS query for the experiment. Some 985,042 experiments (or 26% of the DNS-active experiments) were started, but terminated before any web fetches were executed by the client (the difference between the DNS query log total and the Web query log total). In total some 57% of the placed advertisements produced results that were recorded in the web logs.

A further 1,244,299 experiments, or 44% of all the experiments that contacted the web server, did not complete the experiment and did not download the result URL after 10 seconds, or did not download either of the test URLs within the 10 second wait period before downloading the result URL. Both of these are attributable to the user terminating the advertisement before the download of the test URLs had completed.

This left 1,587,481 experiments that downloaded at least one of the test URLs and communicated their results back to the server on the expiration of the 10 second timer. The `*.d.t5.dotnxdomain.net` is called here "Valid", and the `*.e.t6.dotnxdomain.net` is termed "Invalid". The breakdown of the combination of fetches of these two objects is as follows:

Web Queries:	Valid AND Invalid	1,438,291	90%
	Valid and NOT Invalid	90,138	6%
	NOT Valid and Invalid	59,052	4%

There were 1,438,291 experiments that download both the DNSSEC-valid and invalid URLs, or 90% of the completed experiments. Some 90,138 experiments, or 6% of the total set of completed experiments that loaded the DNSSEC-Valid URL and did not download the DNSSEC-invalid URL. However, there were a further 59,052 experiments, or 4% of the total set, that behaved contrary to DNSSEC, downloading the DNSSEC-invalid URL, but not downloading the DNSSEC-valid URL.

This data points to some considerable level of variability in browser behavior. All these experiments reported back after 10 seconds as to their status, but it appears that some clients (at least 4%) are taking longer than 10 seconds to complete the 2 download tasks, and the experiment was terminated by the user prior to the completion of the experiment. If the number of incomplete experiments is equally distributed between the two cases of retrieving one but not the other URL, then it appears to indicate that some 2% of experiments did not download the DNSSEC-invalid URL because of the negative DNSSEC-validation outcome, while the other 4% did not perform the download because the experiment did not run to completion. However, this does not appear to be a very satisfactory form of analysis for the numbers, and the 2% outcome of DNSSEC-validating users appears to be a highly approximate calculation.

Is there a way to interpret the log files to provide a better estimate of DNSSEC use in the Internet?

Resolvers and DNSSEC Validation

A more methodical approach is to work through the DNS logs to see if we can assemble the set of DNSSEC-validating resolvers, then compare this proposed set to the web logs to see if the web logs contradict the tentative results from the DNS log analysis.

So the first question is: How can we tell if a DNS resolver is performing DNSSEC validation?

This is an example of the log from the local DNS authoritative name server when a DNSSEC-validating resolver generates queries for the experiment

```
15:50:27.130 queries: client 68.x.y.z#62436 (t10000.u1675001815.s1347893426.i767.v6022.d.t5.dotnxdomain.net):
    query: t10000.u1675001815.s1347893426.i767.v6022.d.t5.dotnxdomain.net IN A -ED
15:50:27.327 queries: client 68.x.y.z#45855 (t5.dotnxdomain.net): query: t5.dotnxdomain.net IN DS -ED
15:50:27.523 queries: client 68.x.y.z#45824 (t5.dotnxdomain.net): query: t5.dotnxdomain.net IN DNSKEY -ED
15:50:27.720 queries: client 68.x.y.z#47318 (dotnxdomain.net): query: dotnxdomain.net IN DNSKEY -ED
```

When the client performs the initial A query with the EDNS0 and DO bits set then the response will include the requested A RR, but will also include the RRSIG RRs, or the signature data, and also the relevant NSEC records and their signatures. The client will then attempt to validate these signatures, and to do so it needs the signing key values, or DNSKEY RR values for the domain. To validate this DNSKEY record it will need the DS RRs for the subdomain, obtained from the parent zone. To validate the RRSIG entries that were retrieved in the DS query it will then need the DNSKEY of the parent zone. This will, in turn, require a fetch of the DS RRs from its parent zone, and so on to the root zone.

The inference to be drawn from the logs of this instance of the test is that if a client is using a DNSSEC-validating DNS resolver, then we should see a DNSKEY query from the resolver.

However it is possible for resolvers to be "chained" so that a number of resolvers can lie behind a resolver (as shown in Figure 1). In such a case the "hidden" validating resolver will generate a DNSKEY query, which will be forwarded through a common Non-validating resolver as a distinct query. If we are using a single rule that a visible Validating Resolver generates DNSKEY queries then we will falsely assume that the common non-validating resolver is a DNSSEC-validating resolver. Is there a way to distinguish between these forms of resolver configurations?

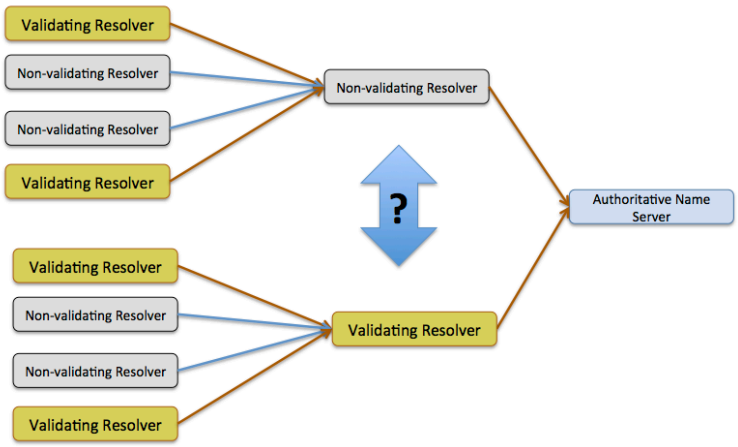

Figure 1 – DNS resolver chaining

The first approach to perform this differentiation of resolver types is to look at the time difference between the first query seen from a resolver and the first DNSKEY query. If the resolver that is querying the authoritative nameservers is itself a DNSSEC-validating resolver then a DNSKEY query will follow the A query "almost immediately", while the non-validating resolver will only pass on the DNSKEY query when a "hidden" DNSSEC-validating resolver performs DNSSEC validation.

The distribution of the elapsed time between the first query seen from each resolver and the DNSKEY query is shown in the following figure. The figure shows a pronounced peak at a delay of 200ms (the x axis uses a logarithmic scale in this figure), and there is a visible waning after 3 seconds.

This allows us to refine our assumptions of how to distinguish between a visible DNSSEC-validating resolver and a non-validating resolver to include the consideration that a DNSSEC validating resolver should query for a DNSKEY RR for the `dotnxdomain.net` domain within 3 seconds of the first query seen from this resolver.

In this experiment we saw 126,780 resolvers, and while 3,367 resolvers performed DNSKEY queries, only 2,277 performed this query within 3 seconds of the resolver's initial query. It seems reasonable to conclude that the remaining 1,090 visible resolvers are non-DNSSEC validating resolvers that may have DNSSEC-validating resolvers chained behind them in some manner.

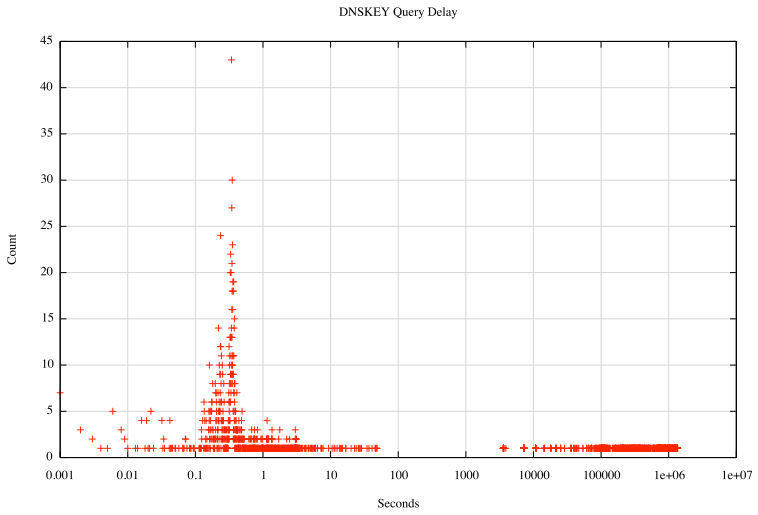

Figure 2 – Distribution of Elapsed time between initial query and DNSKEY query

There is a second filter we can use as well to apply to this candidate set of DNSSEC-validating resolvers. If we look at the each individual experiment (using the unique id generated for each experiment), the DNS logs will reveal which resolvers were used by the end host to resolve the experiment's domain names into IPv4 addresses. DNSSEC-validating resolvers do not return the requested resource record in the case of DNSSEC validation failure. Instead. they return a SERVFAIL error code.

At this stage we have a set of 2,277 visible resolvers whom we suspect are DNSSEC-validating resolvers. We also have a collection of 1,497,343 experiments where the invalid URL was retrieved by the client. If we filter these experiments, and select only those experiments where the client used a single DNS resolver, and further filter this set to retrieve only those experiments where this client loaded the invalid URL, then we have grounds to believe that this single resolver is not a DNSSEC-validating resolver. Some 154 visible DNS resolvers fall into this category.

We now have 2,123 visible DNS resolvers that appear to be performing DNSSEC validation out of a total of 126,780 visible DNS resolvers, or some 1.6% of all visible resolvers.

The initial estimate of 2,316 DNSSEC-validating resolvers out of a total pool of 57,267, or 4.0% of visible resolvers was somewhat optimistic. A revised estimate is somewhat lower, with 2,123 DNSSEC-validating resolvers seen, from a total pool of 126,780 visible resolvers.

What proportion of DNS resolvers are DNSSEC-capable?

2,123 out of 126,780, or 1.7% of the visible DNS resolvers were observed to perform DNSSEC validation

We can also look at the location of these DNS resolvers in terns of the country in which they are located. The Regional Internet Registries all regularly publish address allocation summary reports that

include a mapping of IP address to country code. This allows us to map the IP address of the DNS resolver to a country where the address has been associated from the RIRs' reports. There are a large number of resolvers used by just 1 or 2 client systems, and a smaller number of resolvers used in some form of infrastructure mode where many clients use the same resolver. It appears reasonable to weight each resolver's DNSSEC validating capability by the number of unique clients seen who use that resolver, and use the DNSSC validating resolver weighted count as a percentage of the total weighted resolver draft for each country. From this data we can color a map of the world with the amount of DNSSEC-validating resolvers in each country, as show in Figure 3, below. (The data used to generate this map can be found at http://labs.apnic.net/dnssec/resolvers_by_cc_2.txt). The 10 countries with the highest levels of weighted DNSSEC resolvers are shown in Table 1. It should be noted that while the experiment covered some 750,000 individual experiments, the distribution of the clients who executed this test was not uniformly spread across all countries. The level of uncertainty in the per country data varies according to the number of tests that were performed by clients in each of these countries.

Rank	Resolvers	DNSSEC Resolvers	Client Calls	DNSSEC Clients	DNSSEC Ratio	CC	Country
1	582	97	24785	20592	83%	SE	Sweden
2	34	3	1193	495	41%	AO	Angola
3	374	14	28689	11355	39%	IE	Ireland
4	456	12	24026	9010	37%	CL	Chile
5	76	4	1401	506	36%	ZM	Zambia
6	1301	194	14422	4529	31%	CZ	Czech Republic
7	710	28	15100	3924	25%	ZA	South Africa
8	40	2	1099	215	19%	KG	Kyrgyzstan
9	140	5	3741	693	18%	LU	Luxembourg
10	99	2	19070	3448	18%	MT	Malta
11	440	18	7321	1217	16%	FI	Finland
12	121	1	12034	1849	15%	PR	Puerto Rico
13	428	7	27137	3801	14%	NZ	New Zealand
14	254	6	12047	1607	13%	SI	Slovenia
15	24640	380	1320940	142958	10%	US	United States of America

Table 1 – Ranking of 15 Countries with the highest DNSSEC Resolver capability (Countries with >= 1000 experiment ids)

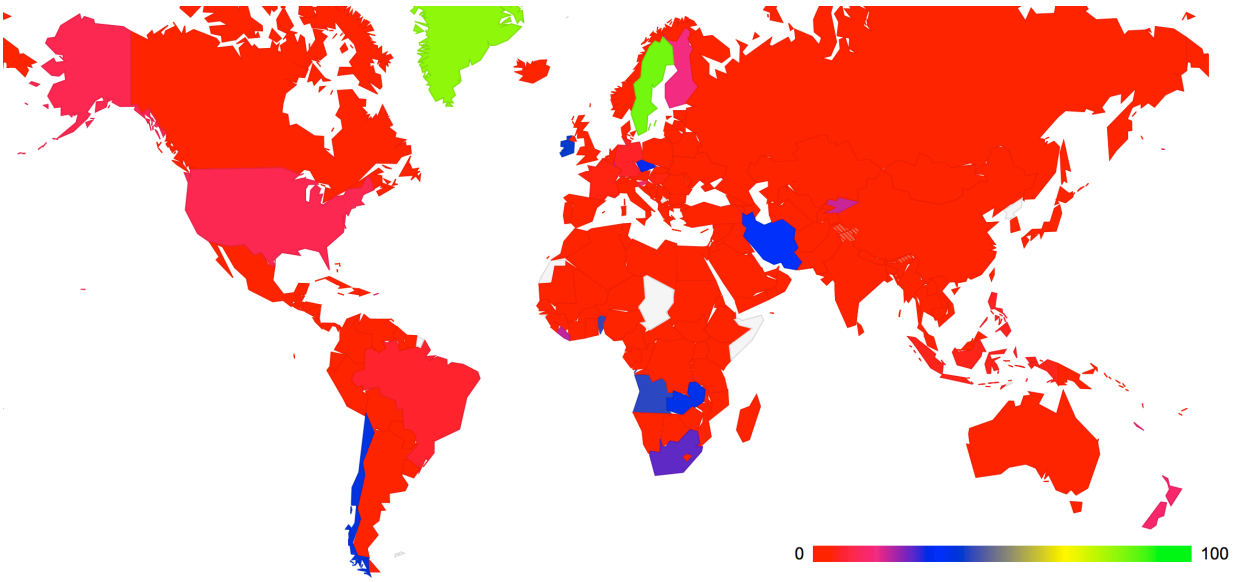

Figure 3: Proportion of Resolvers that Perform DNSSEC Validation by country (weighted by the number of clients who use each resolver)

What about the very largest of these DNS resolvers? The following table lists these largest resolvers and their ability to perform DNSSEC validation. Of the largest 26 individual resolvers we saw in this exercise just 1 set of these resolvers that undertook DNSSEC validation, located in AS7922, and operated by Comcast.

DNSSEC?	Client Count	Origin AS	AS Name	Country
no	976241	AS4766	KIXS-AS-KR Korea Telecom	Republic of Korea
no	472735	AS15169	GOOGLE - Google Inc.	USA
no	411220	AS16880	Trend Micro	USA
no	330663	AS3462	HINET Data Communication Business Group	Taiwan
no	294053	AS3786	LGDACOM LG DACOM Corporation	Republic of Korea
no	274418	AS5384	Emirates Telecommunications	United Arab Emirates
no	228905	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
no	194865	AS9318	HANARO-AS Hanaro Telecom Inc.	Republic of Korea
no	145429	AS4837	CHINA169-BACKBONE CNCGROUP China169	China
yes	140211	AS7922	Comcast Cable Communications	USA
no	120063	AS4788	TM Net, Internet Service Provider	Malaysia
no	113965	AS3356	LEVEL3 Level 3 Communications	US
no	107524	AS9050	RTD ROMTELECOM S.A	Romania
no	100527	AS45595	PKTELECOM-AS-PK Pakistan Telecom Company	Pakistan
no	87825	AS6799	OTENET-GR (Hellenic Telecommunications)	Greece
no	86182	AS7470	TRUEINTERNET-AS-AP TRUE INTERNET Co.,Ltd.	Thailand
no	85917	AS17676	GIGAINFRA Softbank BB Corp.	Japan
no	83349	AS4713	OCN NTT Communications Corporation	Japan
no	82338	AS25019	SAUDINETSTC-AS	Saudi Arabia
no	82146	AS8781	QA-ISP Qatar Telecom (Qtel) Q.S.C.	Qatar
no	78339	AS9737	TOTNET-TH-AS-AP TOT Public Company Limited	Thailand
no	75510	AS9299	Philippine Long Distance Telephone	Philippines
no	71499	AS15557	LDCOMNET Societe Francaise Radiotelephone	France
no	69071	AS45758	TRIPLETNET-AS-AP TripleT Interne	Thailand
no	67079	AS8452	TE-AS TE-AS	Egypt
no	58219	AS36692	OPENDNS - OpenDNS, LLC	USA

Table 2 – Ranking of 26 Largest DNS Resolvers by their DNSSEC Resolver capability

The next table shows the 20 largest DNSSEC-validating resolvers.

DNSSEC?	Client Count	Origin AS	AS Name	Country
yes	140211	AS7922	COMCAST-7922 - Comcast Cable Communication	USA
yes	11355	AS5466	EIRCOM Eircom Limited	Ireland
yes	9327	AS3301	TELIANET-SWEDEN TeliaSonera AB	Sweden
yes	9005	AS22047	VTR BANDA ANCHA S.A.	Chile
yes	7390	AS16276	OVH OVH Systems	France
yes	5313	AS28573	NET Servicos de Comunicao S.A.	Brazil
yes	4758	AS1257	TELE2	European Union
yes	3762	AS7657	VODAFONE-NZ-NGN-AS Vodafone NZ Ltd.	New Zealand
yes	3684	AS23700	BM-AS-ID PT. Broadband Multimedia, Tbk	Indonesia
yes	3649	AS5713	SAIX-NET	South Africa
yes	3448	AS15735	DATASTREAM-NET GO p.l.c.	Malta
yes	3411	AS2519	VECTANT VECTANT Ltd.	Japan
yes	3177	AS29562	KABELBW-ASN Kabel BW GmbH	Germany
yes	2927	AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	China
yes	2180	AS28725	CZ-EUROTEL-AS AS of Eurotel Praha	Czech Republic
yes	1897	AS39651	COMHEM-SWEDEN Com Hem Sweden	Sweden
yes	1849	AS11992	CENTENNIAL-PR - Centennial de Puerto Rico	Puerto Rico
yes	1832	AS12912	ERA Polska Telefonia Cyfrowa S.A.	Poland
yes	1809	AS12301	INVITEL Invitel Tavkozlesi Zrt.	Hungary
Yes	1798	AS11814	DISTRIBUTEL COMMUNICATIONS	Canada

Table 3 – Ranking of 20 Largest DNSSEC-Validating Resolvers y

The full list of the resolvers' DNSSEC capability, per originating AS number can be found at http://labs.apnic.net/dnssec/resolvers_by_origin_as.txt. Of note is the diversity of countries in this list.

Counting Clients

Let's now turn our attention from the resolvers to those clients who use these resolvers, and look at the clients and DNSSEC The web logs allow us to link the resolvers' DNSSEC capability to individual end host systems. This allows us to derive a measurement of the level of coverage of DNSSEC validation capability for end users. In the previous report we took the optimistic view that if any of the resolvers used by a client appeared to perform DNSSEC validation then we were prepared to list the client as performing DNSSEC validation. This resulted in a measurement of 69,560 out of 770,934 experiments, or 9.0% of the clients. We can improve this definition by taking a stricter view, namely what proportion of clients are seen to use only those resolvers that perform DNSSEC-validation. This is similar to the question of what proportion of clients will be unable to load a URL where the DNS label fails DNSSEC validation. As indicated at the start of this article the web logs indicate that some 6% of clients load the DNSSEC-valid URL but do not load the DNSSEC-invalid URL. But, also as noted above, the browser behavior introduces a significant level of uncertainty into these results, and the clients that appear to obey DNSSEC-validation outcomes use a mix of resolvers that both do and do not appear to perform DNSSEC validation.

Perhaps the question can be rephrased differently: What proportion of clients exclusively use DNSSEC-validating resolvers:

What proportion of users are using DNSSEC-validating DNS resolvers?

27,838 out of 1,717,906, or 1.6% of the end host systems were observed to perform DNSSEC validation.

The final query relates to the location of the users. for this experiment we used the mapping of IP address to country codes as published by the RIRs and were able to map users to countries.

Where are these users?

Of the 207 unique country codes that were seen in this experiment, some 105 countries contributed 1000 or more experiments. The 25 countries that contributed 1,000 or more experiments with the highest proportion of DNSSEC use is shown in the following table:

% DNSSEC-Validating Users	DNSSEC Users	DNSSEC Experiments	Country
59.48%	1,982	3,332	Sweden
25.17%	1,632	6,484	Ireland
24.88%	2,068	8,313	Chile
21.95%	570	2,597	Puerto Rico
21.40%	782	3,655	South Africa
15.75%	9,149	58,074	United States of America
14.74%	858	5,820	Czech Republic
7.07%	569	8,045	New Zealand
6.79%	1,917	28,228	Italy
4.82%	171	3,545	Malta
4.69%	93	1,981	Finland
3.75%	171	4,562	Switzerland
3.37%	1,411	41,906	Brazil
2.83%	484	17,105	Germany
2.09%	329	15,711	Ukraine
1.98%	543	27,405	Canada
1.97%	62	3,140	Slovakia
1.89%	799	42,284	Poland

1.65%	792	48,089	Japan
1.65%	255	15,432	Hungary
1.41%	35	2,485	Uruguay
1.21%	105	8,658	Lithuania
1.15%	73	6,331	Colombia
1.15%	41	3,573	Slovenia
1.11%	133	11,963	Serbia

Table 4 – Ranking of 25 Countries with the highest DNSSEC client use

Once again is it possible to feed this data into a map of the world and paint each country with a color that denotes the level of coverage of DNSSEC. This is shown in Figure 4. (The data used to generate this map can be found at http://labs.apnic.net/dnssec/hosts_by_cc_2.txt)

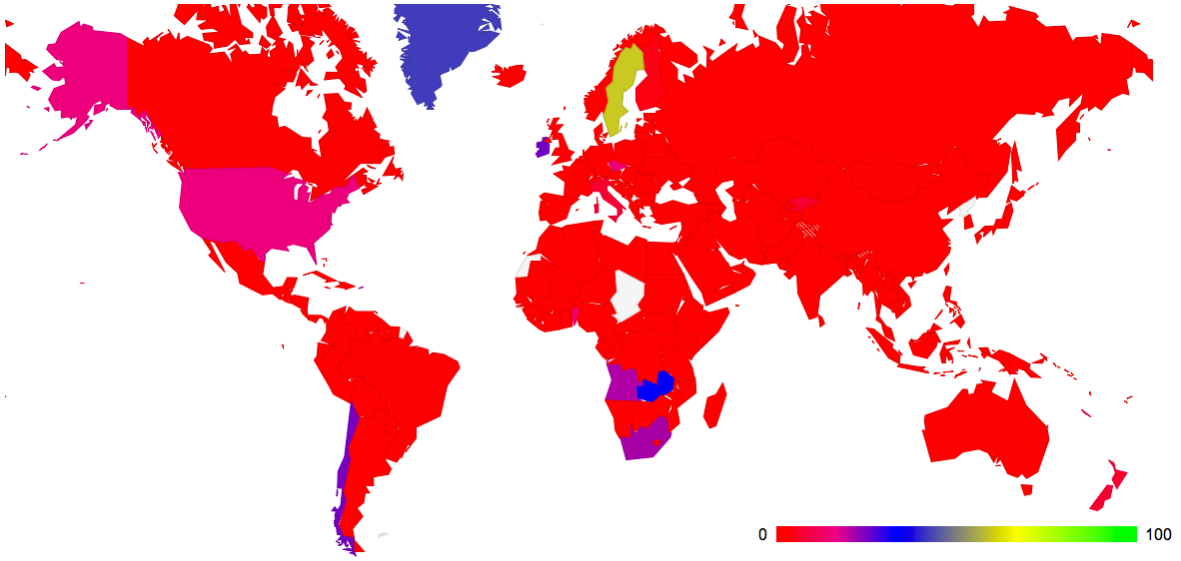

Figure 4: Proportion of Users that use DNSSEC-Validating Resolvers by country

Rather than by country it is also possible to generate the list of DNSSEC-using clients by originating AS. Using a filter of obtaining a minimum of 50 tested clients per originating AS, we obtain the following table of the 25 AS's that have the highest proportion of DNSSEC-using clients.

Rank	AS	DNSSEC Use	DNSSEC Users	Users	AS Name
1	AS44143	97.54%	119	122	VIPMOBILE-AS Vip mobile d.o.o., Serbia
2	AS27831	97.26%	71	73	Colombia Movil, Colombia
3	AS44034	97.03%	261	269	HI3G Hi3G Access AB, Sweden
4	AS28725	96.83%	61	63	CZ-EUROTEL-AS AS of Eurotel Praha, Czech Republic
5	AS15600	96.49%	55	57	FINECOM Finecom Telecommunications AG, Switzerland
6	AS20776	96.26%	180	187	OUTREMER-AS Outremer Telecom, France
7	AS12912	94.93%	712	750	ERA Polska Telefonia Cyfrowa S.A., Poland
8	AS31343	94.30%	248	263	INTERTELECOM Intertelecom Ltd, Ukraine
9	AS29518	91.87%	113	123	BREDBAND2 Bredband2 AB, Sweden
10	AS5466	90.86%	1631	1795	EIRCOM Eircom Limited, Ireland
11	AS38484	90.79%	69	76	VIRGIN-BROADBAND-AS-AP Virgin Broadband VISP, Australia
12	AS22047	88.06%	2066	2346	VTR BANDA ANCHA S.A., Chile
13	AS11992	87.83%	570	649	CENTENNIAL-PR - Centennial de Puerto Rico, Puerto Rico
14	AS3737	87.74%	93	106	PTD-AS - PenTeleData Inc., United States of America
15	AS17711	87.40%	111	127	NDHU-TW National Dong Hwa University, Taiwan
16	AS3301	86.25%	508	589	TELIANET-SWEDEN TeliaSonera AB, Sweden
17	AS3245	85.19%	46	54	DIGSYS-AS Digital Systems Ltd, Bulgaria
18	AS41833	83.78%	62	74	MOSCANET Moscanet (WISE), Lebanon
19	AS8473	82.26%	102	124	BAHNHOF Bahnhof Internet AB, Sweden
20	AS7922	80.43%	8855	11010	COMCAST-7922 - Comcast Cable Communications, Inc., USA

21	AS4704	80.27%	118	147	SANYO Information Technology Solutions Co., Ltd., Japan
22	AS5713	80.09%	744	929	SAIX-NET, South Africa
23	AS41749	80.00%	100	125	NETCOMPUTERS-AS Net & Computers SRL, Romania
24	AS24852	79.44%	85	107	VINITA VINITA Internet Services, Lithuania
25	AS1257	76.16%	409	537	TELE2, European Union

Table 5 – Ranking of 25 ASs with the highest DNSSEC client use

The complete set of data of DNSSEC use by hosts per originating AS can be found at http://labs.apnic.net/dnssec/hosts_by_as_2.txt

Conclusions

Where are we with DNSSEC?

While the most optimistic estimate is that some 9% of clients use a collection of DNS resolvers where one or more of this resolver set appear to undertake DNSSEC validation, if we make the qualifying conditions a little more precise we get a different number.

If the qualifying condition is one to count the proportion Internet clients that are served by exclusively by DNSSEC-validating resolvers, such that a DNSSEC-invalid result will not be passed to the client by any of its configured DNS resolvers, then it appears that just some 1.6% of the Internet's end client population appear to be "protected" by DNSSEC validation.

Disclaimer

About the Author

Geoff Huston B.Sc., M.Sc., 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 has been active in the Internet Engineering Task Force for many years.

www.potaroo.net