The ISP Column
A monthly column on things Internet

October 2012

Geoff Huston,
George Michaelson

Counting DNSSEC

At the Nordunet 2012 conference[1] in September, a presentation[2] included the assertion that "more than 80% of domains could use DNSSEC if they so chose." This is an interesting claim that speaks to a very rapid rise in the deployment of DNSSEC in recent years, and it raises many questions about the overall status of DNSSEC deployment in today's Internet. While the effort to secure the operation of the DNS dates back for more than 10 years[3], the recent impetus for DNSSEC adoption appears to have come from the acknowledgement of vulnerabilities in the DNS with the widespread publication of a viable form of attack on DNS resolvers (the "Kaminsky DNS attack", reported in 2008[4]), and DNSSEC-signed DNS root zone, which commenced on 15 July 2010. The question now is: how is all this playing out in the world of the DNS? How many DNS zones are DNSSEC-signed? To what extent are Internet user's able to trust in the integrity of DNS name resolution? How many Internet users use DNS resolvers that perform DNSSEC validation?

There are certainly a number of very positive individual stories about the extent of DNSSEC adoption. In a recent announcement[5] the operator of the Netherlands ccTLD reported more than 1 million DNSSEC-signed domain name delegations, which is reported to make `.nl` the TLD with the most signed delegations.[6] On a more general level we are aware at in September 2012 some 64 country code Top Level Domains (ccTLD) are DNSSEC-signed, as are many of the generic TLDS (gTLDs) including .com, .net and .org.

But are there some more general questions about the adoption of DNSSEC that we could answer by various forms of direct measurement across the entirety of the Internet? Perhaps if we could undertake a measurement exercise that could answer some, or even all, of the following questions, then we'd have a better idea as to the extent to which DNSSEC is available and being used in today's Internet:

- How many zones are DNSSEC signed?
- How many DNS queries are DNSSEC-validated?
- How many DNS resolvers are DNSSEC-capable?
- How many users are using DNSSEC-aware DNS resolvers?

Of course answering these questions is not necessarily easy. Lets look at each of these questions and see if it is feasible to undertake a measurement exercise that could provide an answer.

---

[1] https://events.nordu.net/display/ndn2012web/Programme
[2] https://events.nordu.net/display/ndn2012web/DNSSEC%3A+from+root+to+%28brown%29+leaves%3A+Lessons+learned+from+4+years+of+active+deployment+-+2
[3] Previous articles on DNSSEC include:
DNSSEC – The Theory - http://www.potaroo.net/ispcol/2006-08/dnssec.html
DNSSEC – The Practice - http://www.potaroo.net/ispcol/2006-09/dnssec2.html
DNSSEC – The Opinion - http://www.potaroo.net/ispcol/2006-10/dnssec3.html
DNSSEC – A Review - http://www.potaroo.net/ispcol/2010-06/dnssec.html
[4] http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug
[5] https://www.sidn.nl/en/news/news/article/more-than-one-million-nl-domain-names-secured-with-dnssec/
[6] http://xs.powerdns.com/dnssec-nl-graph

How many zones are DNSSEC signed?

While individual DNS zone operators may be able to infer amount of DNSSEC use in their local zone, through registration of the DS resource records (RRs), compiling the total picture across all zones is challenging. Zone walking across many domains has not been possible for many years, so to assemble the picture of the totality of the DNS name universe and then count the population of the subset that uses DNSSEC is not really an easy question to answer at the level of the entire namespace of the DNS.

How many DNS queries are DNSSEC-validated?

Again, the problem lies in trying the get a sufficiently broad view of the world. The authoritative name servers for some of the more popular gTLDs and the larger ccTLDs may be able to provide some sample data that would be indicative of the total picture, but if you are not an operator of such a zone this is a tough question to answer. Equally the operator of a recursive DNS resolver, or a DNS Forwarder, for a large population of end user clients could provide direct information about the resolver's clients, but that does not generally extrapolate to a more general picture.

How many DNS resolvers are DNSSEC-capable?

Again this is a difficult question to answer, due to the challenge involved in trying to discover all the DNS resolvers out there, and then generating the conditions that would expose their capability to perform a DNSSEC validation.

How many users are using DNSSEC-aware DNS resolvers?

Again this is a difficult question to answer, due to the challenge involved in trying to get all users to perform a DNS resolution that would allow a data collector to collate all these attempts and produce a picture for the entire internet.

If these questions appear to be challenging, then perhaps it is worth looking around to see if there are meaningful questions could we answer about DNSSEC deployment? If we relax the constraint a little bit and talk about proportions rather than absolute counts, then maybe we could look at ways to generate answers. In this article I will describe an approach we've already used in a number of different contexts[7], and see if we can provide answers to three basic questions about the state of DNSSEC use in the Internet today:

- What proportion of DNS resolvers are DNSSEC-capable?
- What proportion of users are using DNSSEC-validatingDNS resolvers?
- Where are these users?

These are questions that relate to end users and the integrity of the service that is delivered to end users, rather than about domain zones per se. In other words, these are questions about the use of DNSSEC as distinct from questions about the extent to which domains are DNSSEC signed. In economic terms you could say that we are looking at the demand side and not at the supply side of DNSSEC.

[7] Bogon Filter Detection - http://www.potaroo.net/ispcol/2012-02/bogonfilter.html
Measuring IPv6 Country by Country - http://www.potaroo.net/ispcol/2012-07/v6report.html

Measurement Technique

This exercise used an online advertisement delivery system as a means of enrolling end user systems to perform a simple DNSSEC capability experiment. Many online ad systems support dynamic content, and in this case Flash coding was used with the advertisement content to perform the necessary dynamic support for the measurement exercise. We configured the ad to generate two unique URLs and get the user's browser to perform a GET.

The URLs are of the form:

```
http://t10000.u5951826831.s1347594696.i767.v6022.d.t5.<signed domain>.net/1x1.png
```

The 's' and 'u' fields are dynamically generated, and are unique for each user that is presented with an impression of the ad. The combination of these two fields creates an identifier string, which is mapped in to the domain name used to perform the individual retrieval tests. This means that every client will generate a query for resolution of a unique DNS name, so that the caching of the outcome of the DNS query for one instance of this experiment will not carry forward to subsequent end hosts that have been inducted to perform the experiment, even if they may use the same DNS resolver. This configuration implies that for every instance of the experiment that is executed by the end host the authoritative server for the experiment's DNS zone will see a DNS query for resource records for this form of DNS name, and we also expect to see a WEB fetch query for the two URLs that are the measurement experiment.

In this experiment we have used two subdomains, both of which are DNSSEC signed, and each zone consists of a single wildcard, as shown in the following zone configuration file for one of these zones, as shown in Figure 1 (Obviously, the served zone includes the addition of the DNSSEC signature records – the unsigned zone is shown here for simplicity).

```
$TTL 3h
@  IN  SOA  ns1.<signed domain>.net. research.apnic.net. (2012091202 3600 900 1 1 )
   IN  NS  ns1.<signed domain>.net.
   IN  NS  ns2.<signed domain>.net.
   IN  DNSKEY 256 3 5 AwEAAdluSaSH7dPBLmwhihWeo8hY3avgKndK11kqI…
   IN  DNSKEY 257 3 5 AwEAAdoBfmR/NI/1+7jZwngA6PdcdEPVBpx1UjARtX…
*  IN  A  203.133.248.6
```

Figure 1 – A Test Zone Configuration

The only difference between the two subdomains lies in the DNSSEC configuration. In the case of one subdomain the DS records are correctly recorded, while in the case of the other subdomain the DS records are deliberately altered. The intended consequence is that DNSSEC validation of domain names in one subdomain will succeed, while DNSSEC validation in the other subdomain will fail.

The authoritative nameserver for the DNSSEC-signed domains, the nameserver for the two subdomains, the web server and a packet capture process have all been placed on a single platform, allowing the complete set of client transactions that involve DNS name resolution and the subsequent fetch of the web object to be recorded at a single point.

The next step is to enroll a large number of clients from all over the Internet to fetch these two URLs. When the advertisement is shown on a client system as part of the impression of the ad, the dynamic code in the ad generates a unique identifier and the code uses this identifier to construct a URL in each of the two subdomain. The code will then trigger the client to attempt to load these two objects, which, in turn will trigger DNS resolution of these two DNS names. The code will then report back, via a final URL fetch, the success or failure to load the two objects, and the time taken to load each object. All this will occur at the time of the presentation of the ad to the user, and does not require the user's intervention to click on the ad in order to trigger the test sequence.

Analyzing the Logs

The next step is to assemble the information from the various logs into a coherent data set. This is an example of the logs 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._.net):
    query: t10000.u1675001815.s1347893426.i767.v6022.d.t5._.net IN A -ED

15:50:27.327 queries: client 68.x.y.z#45855 (t5._.net): query: t5._.net IN DS -ED

15:50:27.523 queries: client 68.x.y.z#45824 (t5._.net): query: t5._.net IN DNSKEY -ED

15:50:27.720 queries: client 68.x.y.z#47318 (_.net): query: _.net IN DNSKEY -ED
```

This sequence of four DNS queries shows the initial query for an IPv4 address for the experiment "`u1675001815.s134789342`". What follows are three DNS queries that are generated as part of DNSSEC validation process. The resolver queries the local authoritative server for the DS records of the delegated subdomain, and the DNSKEY of the subdomain. The client then queries for the DNSKEY of the domain and it will have queried the .net servers for the corresponding DS records.

```
15:50:28.277 queries: client 68.x.y.z#27401 (t10000.u1675001815.s1347893426.i767.v6022.e.t6._.net):
    query: t10000.u1675001815.s1347893426.i767.v6022.e.t6._.net IN A -ED

15:50:28.474 queries: client 68.x.y.z#49311 (t6._.net): query: t6._.net IN DS -ED

15:50:28.670 queries: client 68.x.y.z#17438 (t6._.net): query: t6._.net IN DNSKEY -ED
```

Here the client queries for the address, and then queries for the DS and DNSKEY records of the subdomain. It does not re-query for the DNSKEY record of the signed domain as it will have cached the response from the previous query.

Following DNS resolution the client will then perform the object fetch. We can then see the subsequent web log entries for the same instance of the experiment:

```
15:50:28 "GET /crossdomain.xml HTTP/1.1" 200 684 1347893428
    t10000.u1675001815.s1347893426.i767.v6022.d.t5._.net

15:50:28 "GET /1x1.png?t10000.u1675001815.s1347893426.i767.v6022.d HTTP/1.1" 200 157 1347893428
    t10000.u1675001815.s1347893426.i767.v6022.d.t5._.net

15:50:37 "GET /1x1.png?t10000.u1675001815.s1347893426.i767.v6022&r=zd-1473.ze-null. HTTP/1.1" 200
    157 1347893437 loggger._.net
```

The client fetches three objects. The first is the "crossdomain.xml" object, to establish permission for fetch objects from a third party domain. The second is the object in the validating subdomain (experiment `d`, in the domain "`d.t5._.net`"). The third is the summary report back from the user, where the inclusion of "`zd-1473`" shows that the client took 1.473 seconds to perform the fetch of the object that had a valid DNSSEC chain. The inclusion of the string "`ze-null`" shows that the client did not retrieve the object in the subdomain "`e.t6._.net`". (This is expected for a DNSSEC-validating resolver, as this `e.t6._.net` is configured with mismatching DS records to cause DNSSEC validation to fail.)

The inference to be drawn from the logs of this instance of the test is that this client is using a DNSSEC-validating DNS resolver, as the resolver fetched the DNSKEY records, and the client did not attempt to fetch the object that was identified with the DNSSEC-invalid domain name.

DNSSEC-Validating Resolvers

This DNSSEC test was active from the 10th to the 17th September 2012.

In that period we recorded 57,268 unique IP addresses querying for A records in the subdomains of the DNSSEC-signed domain name. In other words we observed some 57,268 discrete DNS resolvers.

We also counted the number of unique DNS resolvers that also queried for the DNSKEY RR of the subdomains. Some 2,316 of these resolvers also make this DNSKEY query. Based of this data we can offer an answer to the first of the DNSSEC measurement questions:

What proportion of DNS resolvers are DNSSEC-capable?

2,316 out of 57,267, or 4.0% of the DNS resolvers were observed to perform DNSSEC validation

We also correlated the number of unique experiment identifiers that each resolver queried, and then matched these identifiers with client IP addresses as recorded in the web logs. From this information we were able to calculate the number of distinct client hosts that used each DNS resolver. IN the course of this exercise we noted a significant number of resolvers that were used by 1 or 2 unique clients, and looked at the DNSSEC capabilities of these "small" resolvers, and the corresponding DNSSEC capabilities of the remainder of the resolvers.

There were 40,446 resolvers used by only 1 or 2 unique clients, of which 1,136 were seen to pull the DNSKEY RRs for the subdomains. This results in a proportion of 2.8% of "small" resolvers that perform DNSSEC validation.

There were 16,822 resolvers used by 3 or more unique clients, of which 1,180 were seen to retrieve the DNSKEY RRs. This results in a proportion of 7.0% of "large" resolvers that 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 2, below. (The data used to generate this map can be found at http://labs.apnic.net/dnssec/resolvers_by_cc.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 test that were performed by clients in each of these countries.

Rank	# Resolvers	Avg Clients / Resolver	Weighted % of DNSSEC Resolution	Country
1	3	3	88.89%	Greenland
2	27	4	77.78%	Antigua and Barbuda
3	337	5	73.73%	Sweden
4	15	1	72.22%	Iran
5	8	30	63.22%	Libya
6	705	3	53.65%	Czech Republic
7	135	12	52.53%	Slovenia
8	11	9	52.04%	Equatorial Guinea
9	13350	9	48.57%	United States of America
10	177	6	47.08%	Finland

Table 1 – Ranking of 10 Countries with the highest DNSSEC Resolver capability

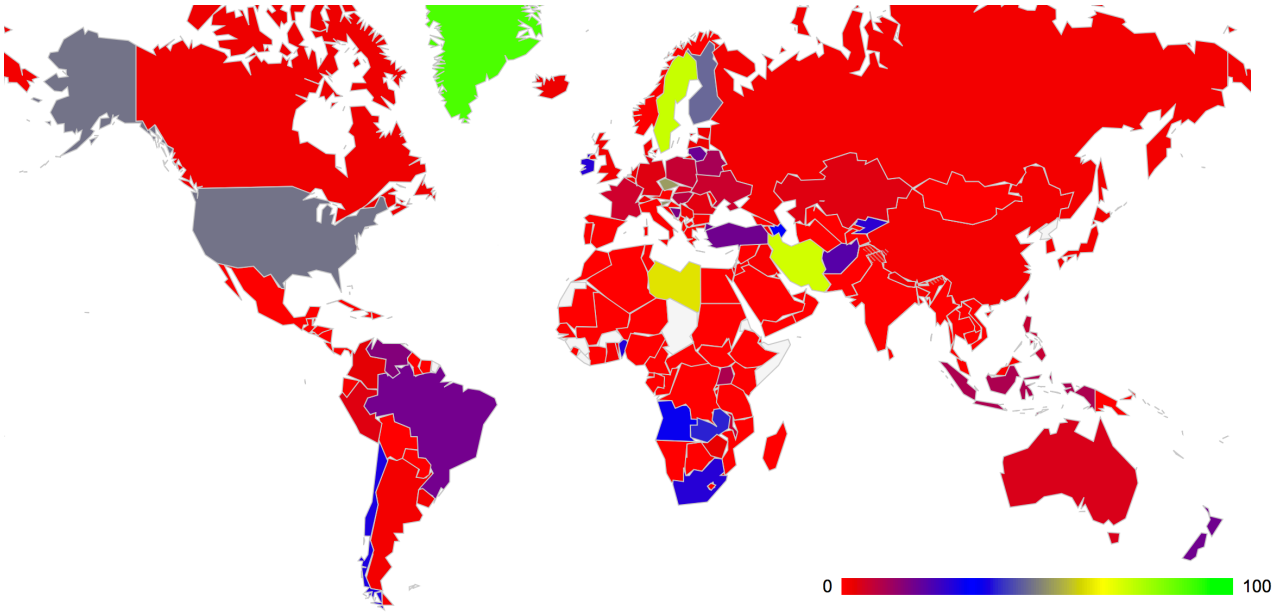

Figure 2: Proportion of Resolvers that Perform DNSSEC Validation by country (weighted by the number of clients who use each resolver)

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 25 individual resolvers we saw in this exercise just 1 set of these resolvers that undertook DNSSEC validation, located in AS 15169, operates by Google.

DNSSEC?	Client Count	AS	AS Name	Country
DNSSEC	47973	AS15169	GOOGLE - Google Inc.	United States of America
no	45990	AS4766	KIXS-AS-KR Korea Telecom	Republic of Korea
no	34213	AS3462	HINET Data Communication Business Group	Taiwan
no	28452	AS3786	LGDACOM LG DACOM Corporation	Republic of Korea
no	25949	AS9318	HANARO-AS Hanaro Telecom Inc.	Republic of Korea
no	21020	AS6799	OTENET-GR (Hellenic Telecommunications Organisation)	Greece
no	16379	AS5384	Emirates Telecommunications Corporation	United Arab Emirates
no	16201	AS45595	PKTELECOM-AS-PK Pakistan Telecom Company Limited	Pakistan
no	16179	AS4134	CHINANET-BACKBONE No.31	China
no	15321	AS25019	SAUDINETSTC-AS SaudiNet	Saudi Arabia
no	11881	AS16880	TRENDMICRO Global IDC and Backbone of Trend Micro	Japan
no	10665	AS4788	TMNET-AS-AP TM Net	Malaysia
no	9595	AS8452	TE-AS TE-AS	Egypt
no	9536	AS3356	LEVEL3 Level 3 Communications	United States of America
no	9232	AS4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	China
no	9210	AS9829	BSNL-NIB National Internet Backbone	India
no	8105	AS15169	GOOGLE - Google Inc.	United States of America
no	7632	AS8781	QA-ISP Qatar Telecom (Qtel) Q.S.C.	Qatar
no	7533	AS6830	LGI-UPC UPC Broadband Holding B.V.	Romania
no	7428	AS24560	Bharti Airtel Ltd. Telemedia Services	India
no	7330	AS4713	OCN NTT Communications Corporation	Japan
no	7196	AS24863	LINKdotNET-AS	Egypt
no	7176	AS36692	OPENDNS - OpenDNS	United States of America
no	6941	AS6866	CYTA-NETWORK Cyprus Telecommunications Authority	Cyprus
no	6898	AS6713	IAM-AS	Morocco

Table 2 – Ranking of 25 Largest DNS Resolvers by their DNSSEC Resolver capability

The full list of the resolvers' DNSSEC capability, per originating AS number can be found at http://labs.apnic.net/dnssec/resolvers_by_as.txt.

It seems that only one DNS service provider, Google, is currently providing DNSSEC validation services to their users from the very largest of the resolver set. At the same time, of the set of resolvers with 1 or 2 clients the number is also low. It would appear that DNSSEC validation is being configured on the mid-sized set of DNS resolvers from this data.

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.

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

69,560 out of 770,934, or 9.0% 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 136 countries contributed 100 or more experiments. The 25 countries with the highest proportion of DNSSEC use is shown in the following table:

Country	%-users	DNSSEC Use	Hosts	GDP per capita
Libya	73%	242	330	$14,100
Sweden	62%	820	1307	$40,900
Czech Republic	56%	1331	2348	$27,400
Slovenia	53%	839	1555	$29,000
Occupied Palestinian Territory	53%	568	1056	
Azerbaijan	49%	760	1522	$10,300
Djibouti	46%	84	181	$ 2,700
Algeria	46%	1510	3268	$ 7,400
Zambia	43%	154	355	$ 1,600
Luxembourg	43%	138	320	$81,100
Brunei Darussalam	42%	92	219	$50,000
Ireland	41%	807	1958	$40,100
Angola	40%	66	162	$ 6,000
Nicaragua	40%	61	152	$ 3,200
Finland	37%	141	375	$36,700
Turkey	34%	1793	5150	$14,700
Guam	34%	47	137	
Kyrgyzstan	32%	43	133	$ 2,400
Vietnam	29%	1003	3371	$ 3,400
Chile	29%	845	2903	$17,400
Dominica	29%	163	562	$14,000
Belarus	28%	352	1215	$15,200
Uganda	28%	181	635	$ 1,300
South Africa	28%	737	2621	$11,100
Indonesia	26%	3633	13921	$ 4,700

Table 3 – Ranking of 25 Countries with the highest DNSSEC client use

What is somewhat surprising here is the variance of these countries in terms of GDP per capita. It is evident that the deployment of DNSSEC is not based on the richer economies, nor in those countries with the longest experience in operating Internet services, but we observe a mix of certain developed, developing and least developed economies providing DNSSEC validation services to their client base.

The other end of the spectrum, those economies with the lowest proportion of DNSSEC validation coverage is show below:

Country	%-users	DNSSEC Use	Hosts	GDP per capita
Costa Rica	2.52%	6	238	$12,100
Uruguay	2.49%	27	1084	$15,300
Georgia	2.45%	36	1472	$ 5,600
Botswana	2.42%	9	372	$16,200
Jordan	2.36%	50	2118	$ 6,000
Saudi Arabia	2.33%	376	16169	$24,500
Croatia	2.30%	117	5077	$18,400
France	2.30%	336	14625	$35,600
Austria	2.18%	177	8113	$42,400
Spain	2.15%	176	8168	$31,000
Netherlands Antilles	2.11%	3	142	
Oman	2.08%	36	1732	$26,900
Cyprus	2.03%	165	8137	$29,400
Republic of Korea	1.89%	1469	77571	$32,100
Mauritius	1.86%	16	859	$15,100
Greece	1.72%	562	32649	$26,600
Kuwait	1.70%	40	2359	$42,200
Macao Special Administrative Region of China	1.56%	11	706	$33,000
El Salvador	1.56%	7	450	$ 7,600
Trinidad and Tobago	1.56%	7	450	$20,300
Dominican Republic	1.46%	20	1369	$ 9,400
United Arab Emirates	0.79%	114	14374	$48,800
Mexico	0.69%	43	6274	$14,800
Qatar	0.51%	37	7263	$104,300
Mongolia	0.47%	1	212	$44,800

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

Again the same mix of developed and developing economies is evident and a similar mix of mature Internet infrastructure and more recent infrastructure deployment is evident here as well.

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 3. (The data used to generate this map can be found at http://labs.apnic.net/dnssec/hosts_by_cc.txt)

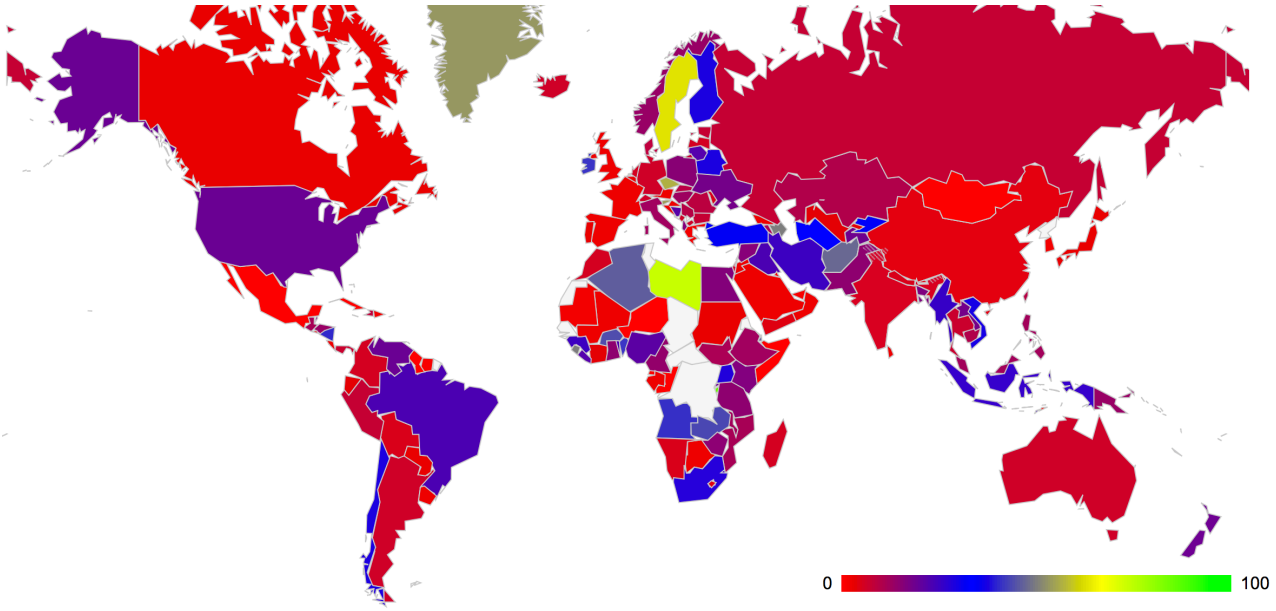

Figure 3: Proportion of Users that use DNSSEC-Validating Resolvers by country

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 20 AS's that have the highest proportion of DNSSEC-using clients.

Rank	AS	DNSSEC Use	DNSSEC Users	Clients Tested	AS Name	Country
1	AS44143	100.00%	67	67	VIPMOBILE-AS Vip mobile d.o.o.	Serbia
2	AS31343	99.18%	121	122	INTERTELECOM Intertelecom Ltd	Ukraine
3	AS198471	98.65%	73	74		Italy
4	AS44034	98.37%	121	123	HI3G Hi3G Access AB	Sweden
5	AS12849	97.53%	79	81	HOTNET-IL Hot-Net internet services Ltd.	Israel
6	AS7657	96.96%	575	593	VODAFONE-NZ-NGN-AS Vodafone NZ Ltd.	New Zealand
7	AS12912	96.88%	186	192	ERA Polska Telefonia Cyfrowa S.A.	Poland
8	AS48161	96.54%	335	347	NG-AS SC NextGen Communications SRL	Romania
9	AS22047	96.15%	800	832	VTR BANDA ANCHA S.A.	Chile
10	AS34779	95.74%	292	305	T-2-AS AS set propagated by T-2	Slovenia
11	AS8473	95.00%	57	60	BAHNHOF Bahnhof Internet AB	Sweden
12	AS29562	95.00%	228	240	KABELBW-ASN Kabel BW GmbH	Germany
13	AS20776	94.37%	67	71	OUTREMER-AS Outremer Telecom	France
14	AS5713	93.84%	533	568	SAIX-NET	South Africa
15	AS5603	93.54%	478	511	SIOL-NET Telekom Slovenije d.d.	Slovenia
16	AS38511	93.01%	133	143	TACHYON-AS-ID PT Remala Abadi	Indonesia
17	AS8767	92.98%	53	57	MNET-AS M-net AS	Germany
18	AS34170	91.93%	205	223	AZTELEKOM Azerbaijan Telecomunication	Azerbaijan
19	AS5610	91.61%	732	799	Telefonica Czech Republic	Czech Rep.
20	AS1759	91.60%	229	250	TSF-IP-CORE TeliaSonera Finland IP Network	Finland

Table 5 – Ranking of 20 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_cc.txt

Conclusions

Where are we with DNSSEC? The good news is that some 9% of the Internet user base appears to be configured with DNS resolvers that perform DNSSEC validation. This is a very encouraging outcome.

On the other hand the very largest of the DNS resolvers, operating as infrastructure servers for the largest of the networks, generally do not perform DNSSEC, with the singularly notable exception of Google's Public DNS Resolver service (https://developers.google.com/speed/public-dns/docs/intro). Across much of the "mature" Internet infrastructure we do not observe much DNSSEC outside of user's who have configured to operate with Google's Public DNS.

We'll return to look at the state of DNSSEC deployment in a few months time, to see what has changed and what has not.

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