# The ISP Column

*A monthly column on things Internet*

June 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, and also learned more about the finer details of Google’s online ad presentation behaviour. But one thing we did not see was any large scale jumps in the level of client use of DNSSEC validation over this period.

This apparent slowness in the adoption of DNSSEC a source of some frustration for many. 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. Obviously, you are now connected to the service you were wanting. But there is the risk that you are not. There is a risk from various forms of so-called “man-in-the-middle” attacks that you have been mislead. Most of such forms of attack pass largely unnoticed. But from time to time they attract a high level of prominence in the public eye, such as the attacks that resulted from Diginotar attack on a Domain Name Certification Authority back in 2011 (<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, firstly, 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 to be embedded into the DNS in a secure manner (as described in RFC6394), which is one potentially effective response to the form of attack we saw as a consequence of the compromise of Diginotar’s CA services.

Attention has been focussed to the effort to deploy DNSSEC in the domain name system. In recent years 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).

At the other end of the spectrum we have seen increasing use of DNSSEC validation in DNS resolution. We 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 2012 we saw some 1.6% of clients exclusively use DNSSEC-validating resolvers, using a relatively coarse measurement methodology.

At the start of 2013 we revised the experiment, and saw some 3% of users appear to exclusively use DNSSEC validating resolvers, and, appropriately, will be unable to resolve a DNS name when its DNSSEC signature is invalid. A further 2% of clients use a mix of DNSSEC-validating and non-validating resolvers.

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 required the client to set the DNSSEC OK (DO) flags on its queries in order to trigger a DNSSEC validation function, 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 with DNSSEC?

### Use of DNSSEC

We ran the experiment across the period of the 9th May through to the 26th May, and ran the test across 2,595,672 clients, selected using an online advertisement placement method.

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 an invalidly-signed DNSSEC signature. All three URLs used a label part that was unique across a minimum of two hours elapsed time, and the DNS records had a TTL of one hour. Through these measures we were trying the minimize any DNS caching, ensuring that all queries were passed to the authoritative name server.

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) |
| no | no | no | 36,527 | 1.4% | 0.6% |
| yes | no | no | 4,501 | 0.5% | 0.1% |
| no | yes | no | 9,253 | 0.4% | 0.1% |
| **yes** | **yes** | **no** | **216,281** | **8.3%** | **3.5%** |
| no | no | yes | 3,582 | 0.1% | 0.1% |
| yes | no | yes | 20,210 | 0.8% | 0.1% |
| no | yes | yes | 12,616 | 0.5% | 0.2% |
| **yes** | **yes** | **yes** | **2,292,702** | **88.3%** | **95.3%** |

*Table 1 – DNSSEC Fetch Results*

If a client supports DNSSEC validation outcomes then it would fetch URLs A and B, but not C. If it does not support DNSSEC validation then it should fetch all three URLs, as in all other respects the three URLs are almost identical. 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.

According to these web logs, within an error bound of ±2% some 8.0% of clients appear to be performing some kind of DNSSEC validation, based on the combinations of URLs that they are able to fetch. This appears to represent 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.

However, a detailed examination of the logs of the DNS authoritative server can provide a better insight into these numbers.

|  |  |  |  |
| --- | --- | --- | --- |
| **Client Behaviour** | **Count** | **%** | **% (Feb 13)** |
| DNSSEC Validating | 210,081 | 8.1% | 3.3% |
| Mix of Resolvers | 213,869 | 8.2% | 2.6% |
| NO DNSSEC | 2,171,722 | 83.7% | 94.1% |

This 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 8.1% 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 5.6%, from 2.6% in February 2013 to 8.2% in May 2013.

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

Of the 2.5M clients who ran this experiment, we saw 184,777 clients use Google Public DNS servers, or 7.15% of all tested clients. Of these, we saw some 101,432, or 3.93% of all clients exclusively use Google’s Public DNS servers, with the remaining 83,345 (or 3.22%) clients use a mix of Google DNS servers and other servers.

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

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Rank | CC | %DNSSEC | %MIXED | %NOT | Samples | Country |
| 1 | SE | 76.37 | 4.60 | 19.02 | 5,367 | Sweden |
| 2 | AG | 58.48 | 8.30 | 33.22 | 289 | Antigua and Barbuda |
| 3 | SI | 57.04 | 6.53 | 36.43 | 4,795 | Slovenia |
| 4 | AO | 46.36 | 21.82 | 31.82 | 220 | Angola |
| 5 | LU | 43.43 | 7.42 | 49.15 | 647 | Luxembourg |
| 6 | FI | 38.71 | 18.40 | 42.89 | 2,364 | Finland |
| 7 | VN | 36.86 | 4.50 | 58.64 | 27,574 | Vietnam |
| 8 | CL | 33.05 | 8.67 | 58.28 | 49,975 | Chile |
| 9 | CZ | 32.77 | 8.68 | 58.54 | 30,905 | Czech Republic |
| 10 | JM | 28.62 | 4.21 | 67.18 | 1,569 | Jamaica |
| 11 | IE | 26.44 | 6.12 | 67.44 | 8,414 | Ireland |
| 12 | NC | 25.76 | 6.44 | 67.80 | 264 | New Caledonia |
| 13 | BB | 24.47 | 1.78 | 73.76 | 1,406 | Barbados |
| 14 | ID | 23.18 | 9.33 | 67.48 | 53,541 | Indonesia |
| 15 | ZA | 21.58 | 10.54 | 67.89 | 2,762 | South Africa |
| 16 | UA | 21.29 | 13.64 | 65.07 | 26,327 | Ukraine |
| 17 | AF | 19.02 | 32.20 | 48.78 | 205 | Afghanistan |
| 18 | TR | 17.97 | 2.43 | 79.60 | 49,762 | Turkey |
| 19 | US | 17.43 | 4.55 | 78.02 | 148,467 | United States of America |
| 20 | BO | 15.83 | 16.85 | 67.32 | 1,478 | Bolivia |

(A full list of all countries and their counts of clients who perform DNSSEC validation can be found at <http://www.potaroo.net:/ispcol/2013-06/dnssec-dnssec_by_country.txt>)

1 39651 96.81 0.83 2.36 721 COMHEM-SWEDEN Com Hem Sweden

2 44034 96.71 1.97 1.32 304 HI3G Hi3G Access AB

3 34525 96.24 1.13 2.63 266 KOBA-AS KoBa Konrad Baranowski

4 22047 95.96 1.55 2.50 16752 VTR BANDA ANCHA S.A.

5 27668 95.94 1.92 2.14 468 ETAPA EP

6 197121 95.72 1.35 2.93 444 DIODOS Greek Research and Technology Network S.A

7 29562 95.34 2.07 2.59 579 KABELBW-ASN Kabel BW GmbH

8 44489 95.31 1.79 2.90 448 STARNET Starnet s.r.o.

9 198471 94.94 2.02 3.03 692 LINKEM-AS Linkem spa

10 34779 94.94 1.08 3.98 830 T-2-AS T-2, d.o.o.

11 52400 94.86 1.37 3.77 292 Olo del Peru S.A.C

12 719 94.37 2.22 3.41 586 ELISA-AS Elisa Oyj

13 44143 94.26 3.55 2.19 366 VIPMOBILE-AS Vip mobile d.o.o.

14 12912 94.14 4.04 1.82 1485 ERA Polska Telefonia Cyfrowa S.A.

15 5603 94.10 2.33 3.57 1372 SIOL-NET Telekom Slovenije d.d.

16 5628 94.04 3.83 2.13 235 EUROTEL-SK Slovak Telecom, a. s.

17 7679 92.24 0.43 7.33 232 QTNET Kyushu Telecommunication Network Co.,Inc.

18 37457 91.31 3.76 4.93 426 Telkom-Internet

19 8473 90.38 4.81 4.81 208 BAHNHOF Bahnhof Internet AB

If we look just a the clients who perform DNSSEC validation, whose DNS resolvers are they using?

Which resolvers do they use?

15169 109466 52.35% 0 44.53% GOOGLE - Google Inc. US United States of America

7922 23009 11.00% 0 10.73% COMCAST-7922 - Comcast Cable Communications, Inc. US United States of America

22047 15953 7.63% 0 7.59% VTR BANDA ANCHA S.A. CL Chile

28573 10966 5.24% 0 5.18% NET Servicos de Comunicao S.A. BR Brazil

28725 5147 2.46% 0 1.94% CZ-EUROTEL-AS AS of Eurotel Praha CZ Czech Republic

6849 4046 1.94% 0 1.83% UKRTELNET JSC UKRTELECOM, UA Ukraine

9299 3738 1.79% 0 1.55% IPG-AS-AP Philippine Long Distance Telephone Company PH Philippines

12301 2783 1.33% 0 1.28% INVITEL Invitel Tavkozlesi Zrt. HU Hungary

5466 1940 0.93% 0 0.92% EIRCOM Eircom Limited IE Ireland

5610 1740 0.83% 0 0.26% TO2-CZECH-REPUBLIC Telefonica Czech Republic, a.s. CZ Czech Republic

Can we quantify google DNS?

    a) clients who exclusively use GOOGLE DNS

    b) clients to fail TO google DNS

    c) clients who fail FROM google DNS

    d) clients who do NOT use GOOGLE DNS

DO bit set



### Disclaimer

The views expressed are the authors’ and not those of APNIC, unless APNIC is specifically identified as the author of the communication. APNIC will not be legally responsible in contract, tort or otherwise for any statement made in this publication.



### 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*](http://www.potaroo.net)