Measuring DNSSEC

Geoff Huston & George Michaelson
APNIC Labs
September 2012

What are the questions?

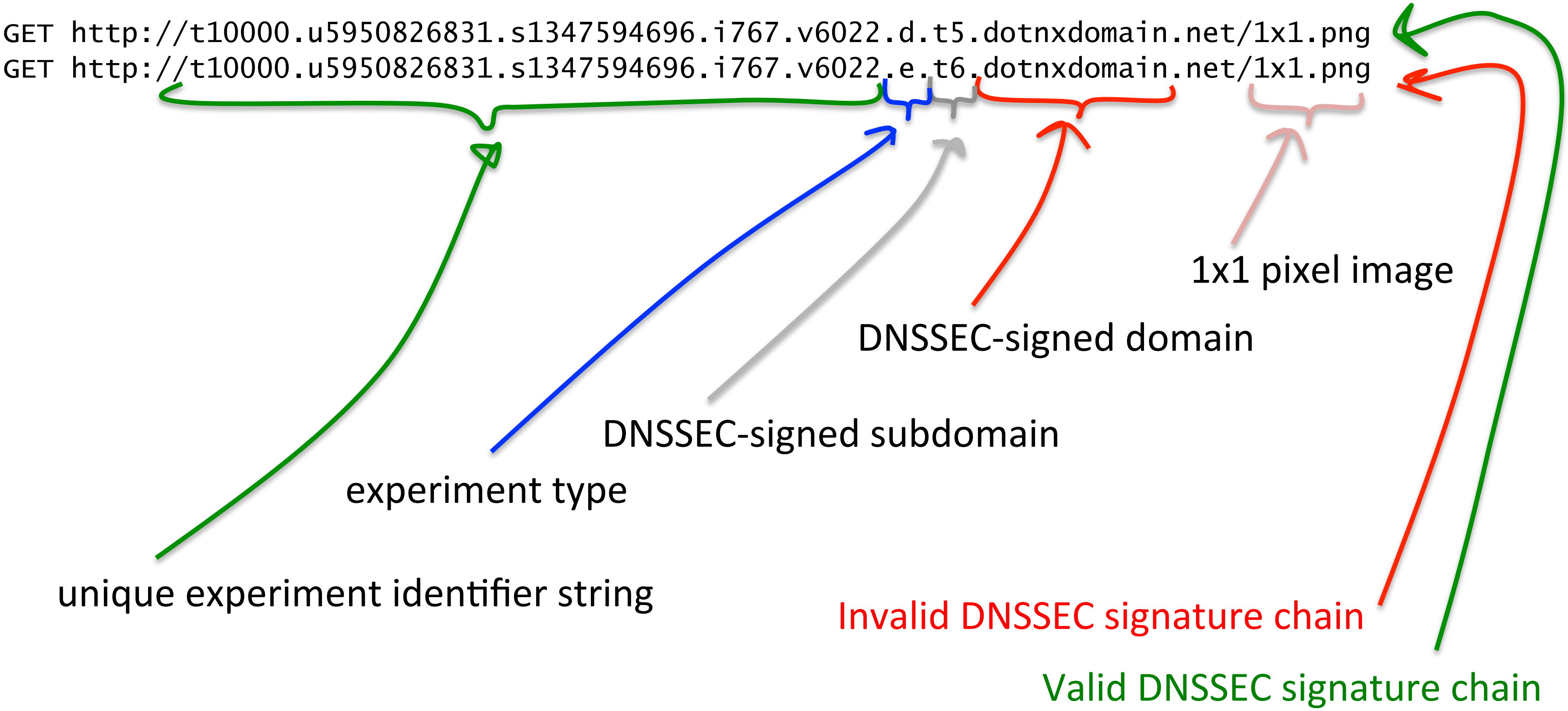
1. What proportion of DNS resolvers are DNSSEC-capable?

2. What proportion of users are using DNSSEC-validatingDNS resolvers?

3. Where are these users?

Experimental Technique

- Use code embedded in an online ad to perform two simple DNSSEC tests



```
GET http://t10000.u5950826831.s1347594696.i767.v6022.d.t5.dotnxdomain.net/1x1.png
GET http://t10000.u5950826831.s1347594696.i767.v6022.e.t6.dotnxdomain.net/1x1.png
```

1x1 pixel image

DNSSEC-signed domain

DNSSEC-signed subdomain

experiment type

unique experiment identifier string

Invalid DNSSEC signature chain

Valid DNSSEC signature chain

The Experiment

- Embed the unique id generation and the ad control in flash code
- Get an online advertisement network to display the ad
- The underlying code and the retrieval of the image is executed as part of the ad display function
  - No click is required!

    (or wanted!)

Experiment Run

10 – 17 September 2012

Resolvers:

- How many unique IP addresses queried for experiment domains in dotnxdomain.net?

- How many of these DNS resolvers also queried for the DNSKEY RR of dotnxdomain.net?

Resolvers:

- How many unique IP addresses queried for experiment domains in dotnxdomain.net?

  57,268

- How many of these DNS resolvers also queried for the DNSKEY RR of dotnxdomain.net?

  2,316

Q1: What proportion of DNS resolvers are DNSSEC-capable?

4.0% of visible DNS resolvers appear to be performing DNSSEC validation

"small scale" Resolvers

How many “small” resolvers were seen: **40,446**

How many perform DNSSEC validation: **1,136**

What’s the DNSSEC-active proportion of these resolvers: **2.8%**

Infrastructure Resolvers:

Filter out all resolvers that are associated with just 1 or 2 end clients

How many resolvers are left: **16,822**

How many perform DNSSEC validation: **1,180**

What’s the DNSSEC-active proportion of these resolvers: **7.0%**

The Biggest Resolvers

DNSSEC?	Clients	AS	AS NAME	Country
yes	**47973**	**AS15169**	**GOOGLE - Google Inc.**	**USA**
no	45990	AS4766	KIXS-AS-KR Korea Telecom	Korea
no	34213	AS3462	HINET Data Communication Business Group	Taiwan
no	28452	AS3786	LGDACOM LG DACOM Corporation	Korea
no	25949	AS9318	HANARO-AS Hanaro Telecom Inc.	Korea
no	21020	AS6799	OTENET-GR (Hellenic Telecommunications)	Greece
no	16379	AS5384	Emirates Telecommunications Corporation	UAE
no	16201	AS45595	PKTELECOM-AS-PK Pakistan Telecom	Pakistan
no	16179	AS4134	CHINANET-BACKBONE No.31	China
no	15321	AS25019	SAUDINETSTC-AS SaudiNet	Saudi Arabia
no	11881	AS16880	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	USA
no	9232	AS4837	CHINA169-BACKBONE CNCGROUP China169	China
no	9210	AS9829	BSNL-NIB National Internet Backbone	India

Now lets look at Clients:

- How many unique IP addresses performed web fetches for objects named in the experiment?

- How many clients used DNS resolvers that also logged queries for the DNSKEY RR of dotnxdomain.net?

Clients:

- How many unique IP addresses performed web fetches for objects named in the experiment?

  770,934

- How many clients used DNS resolvers that also logged queries for the DNSKEY RR of dotnxdomain.net?

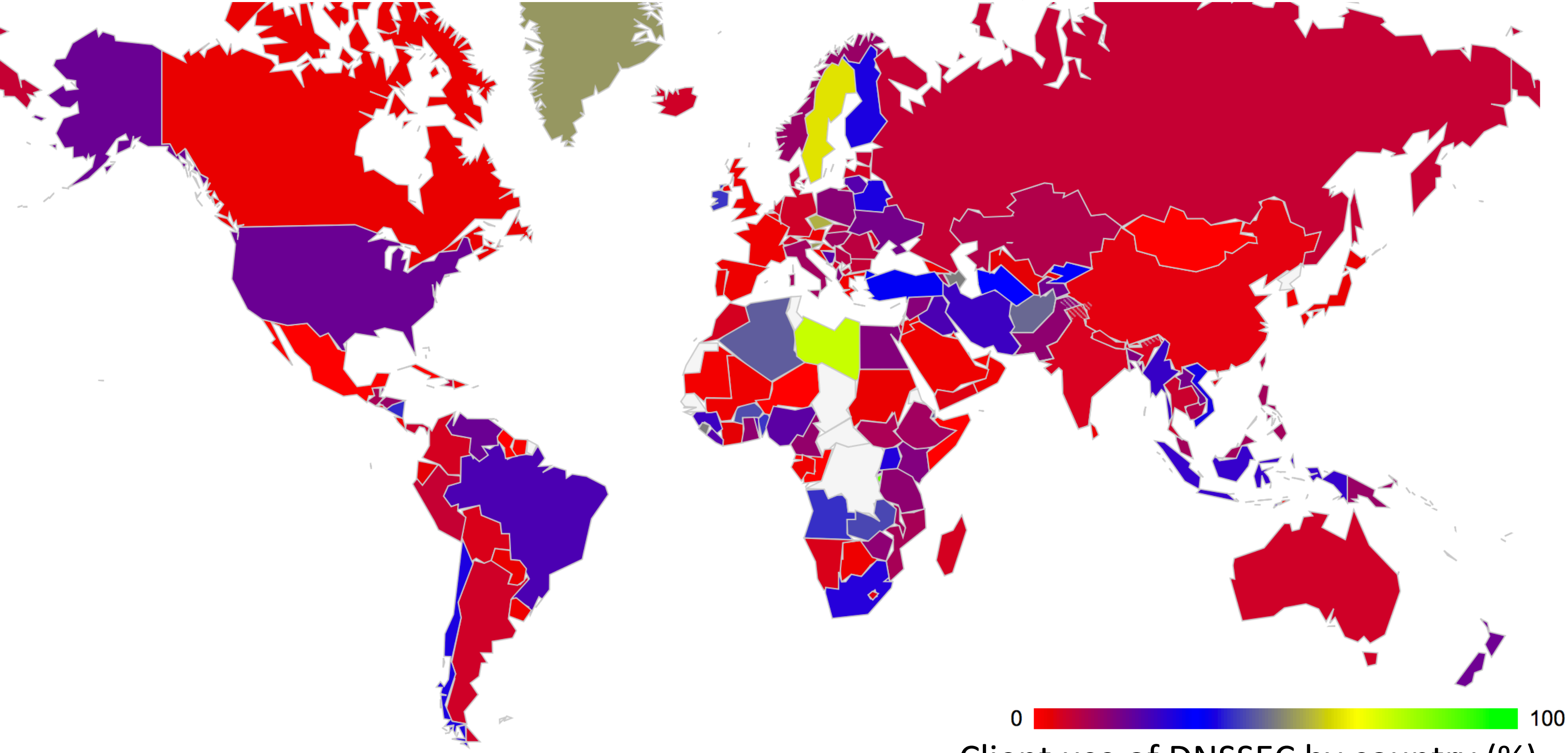
  69,560

Q2: What proportion of users are DNSSEC-validating resolvers?

9.0% of end client systems are using DNS resolvers that appear to be performing DNSSEC validation

Q3: Where can we find DNSSEC-validating users?

Q3: Where can we find DNSSEC-validating users?



Client use of DNSSEC by country (%)
September 2012

The top of the country list

% who	CC	sample client counts		
use		DNSSEC		
DNSSEC			Total	
73.33%	LY	242	330	Libya
62.74%	SE	820	1307	Sweden
56.69%	CZ	1331	2348	Czech Republic
53.95%	SI	839	1555	Slovenia
53.79%	PS	568	1056	Occupied Palestinian Territory
49.93%	AZ	760	1522	Azerbaijan
46.41%	DJ	84	181	Djibouti
46.21%	DZ	1510	3268	Algeria
43.38%	ZM	154	355	Zambia
43.12%	LU	138	320	Luxembourg
42.01%	BN	92	219	Brunei Darussalam
41.22%	IE	807	1958	Ireland
40.74%	AO	66	162	Angola
40.13%	NI	61	152	Nicaragua
37.60%	FI	141	375	Finland
34.82%	TR	1793	5150	Turkey
34.31%	GU	47	137	Guam
32.33%	KG	43	133	Kyrgyzstan
29.75%	VN	1003	3371	Vietnam
29.11%	CL	845	2903	Chile
29.00%	DM	163	562	Dominica
28.97%	BY	352	1215	Belarus
28.50%	UG	181	635	Uganda
28.12%	ZA	737	2621	South Africa
26.10%	ID	3633	13921	Indonesia
25.62%	JM	154	601	Jamaica

Ranking only those countries with more than 100 sample points in this experiment run (136 countries)

And the bottom of the list

% who use DNSSEC	CC	sample client counts		
		DNSSEC	Total	
73.33%	LY	242	330	Libya
62.74%	SE	820	1307	Sweden
56.69%	CZ	1331	2348	Czech Republic
53.95%	SI	839	1555	Slovenia
53.79%	PS	568	1056	Occupied Palestinian Territory
49.93%	AZ	760	1522	Azerbaijan
46.41%	DJ	84	181	Djibouti
46.21%	DZ	1510	3268	Algeria
43.38%	ZM	154	355	Zambia
43.12%	LU	138	320	Luxembourg
42.01%	BN	92	219	Brunei Darussalam
41.22%	IE	807	1958	Ireland
40.74%	AO	66	162	Angola
40.13%	NI	61	152	Nicaragua
37.60%	FI	141	375	Finland
34.82%	TR	1793	5150	Turkey
34.31%	GU	47	137	Guam
32.33%	KG	43	133	Kyrgyzstan
29.75%	VN	1003	3371	Vietnam
29.11%	CL	845	2903	Chile
29.00%	DM	163	562	Dominica
28.97%	BY	352	1215	Belarus
28.50%	UG	181	635	Uganda
28.12%	ZA	737	2621	South Africa
26.10%	ID	3633	13921	Indonesia
25.62%	JM	154	601	Jamaica

% who use DNSSEC	CC	sample client counts		
		DNSSEC	Total	
2.63%	LK	115	4372	Sri Lanka
2.52%	CR	6	238	Costa Rica
2.49%	UY	27	1084	Uruguay
2.45%	GE	36	1472	Georgia
2.42%	BW	9	372	Botswana
2.36%	JO	50	2118	Jordan
2.33%	SA	376	16169	Saudi Arabia
2.30%	HR	117	5077	Croatia
2.30%	FR	336	14625	France
2.18%	AT	177	8113	Austria
2.15%	ES	176	8168	Spain
2.11%	AN	3	142	Netherlands Antilles
2.08%	OM	36	1732	Oman
2.03%	CY	165	8137	Cyprus
1.89%	KR	1469	77571	Republic of Korea
1.86%	MU	16	859	Mauritius
1.72%	GR	562	32649	Greece
1.70%	KW	40	2359	Kuwait
1.56%	MO	11	706	Macao Special Administrative Region of China
1.56%	SV	7	450	El Salvador
1.56%	TT	7	450	Trinidad and Tobago
1.46%	DO	20	1369	Dominican Republic
0.79%	AE	114	14374	United Arab Emirates
0.69%	MX	43	6274	Mexico
0.51%	QA	37	7263	Qatar
0.47%	MN	1	212	Mongolia

Ranking only those countries with more than 100 sample points in this experiment run (136 countries)

DNSSEC-Validating Clients by AS – the top AS's

```
% who  ASN      sample client counts
 use            DNSSEC
DNSSEC               Total

100.00%  44143   67   67  RS VIPMOBILE-AS Vip mobile d.o.o., Serbia
99.18%  31343  121  122  UA INTERTELECOM Intertelecom Ltd, Ukraine
98.65% 198471   73   74  IT , Italy
98.37%  44034  121  123  SE HI3G Hi3G Access AB, Sweden
97.53%  12849   79   81  IL HOTNET-IL Hot-Net internet services Ltd., Israel
96.96%   7657  575  593  NZ VODAFONE-NZ-NGN-AS Vodafone NZ Ltd., New Zealand
96.88%  12912  186  192  PL ERA Polska Telefonia Cyfrowa S.A., Poland
96.54%  48161  335  347  RO NG-AS SC NextGen Communications SRL, Romania
96.15%  22047  800  832  CL VTR BANDA ANCHA S.A., Chile
95.74%  34779  292  305  SI T-2-AS AS set propagated by  T-2, d.o.o., Slovenia
95.00%   8473   57   60  SE BAHNHOF Bahnhof Internet AB, Sweden
95.00%  29562  228  240  DE KABELBW-ASN Kabel BW GmbH, Germany
94.37%  20776   67   71  FR OUTREMER-AS Outremer Telecom, France
93.84%   5713  533  568  ZA SAIX-NET, South Africa
93.54%   5603  478  511  SI SIOL-NET Telekom Slovenije d.d., Slovenia
93.01%  38511  133  143  ID TACHYON-AS-ID PT Remala Abadi, Indonesia
92.98%   8767   53   57  DE MNET-AS M-net AS, Germany
91.93%  34170  205  223  AZ AZTELEKOM Azerbaijan Telecomunication ISP, Azerbaijan
91.61%   5610  732  799  CZ TO2-CZECH-REPUBLIC Telefonica Czech Republic, a.s., Czech Republic
91.60%   1759  229  250  EU TSF-IP-CORE TeliaSonera Finland IP Network, European Union
91.30%   4704   63   69  JP SANNET SANYO Information Technology Solutions Co., Ltd., Japan
91.24%   5466  781  856  IE EIRCOM Eircom Limited, Ireland
90.32%  39725   56   62  KZ DTVKZ-AS Digital TV, LLP, Kazakhstan
90.08%   7922 4578 5082  US COMCAST-7922 - Comcast Cable Communications, Inc., United States of America
90.00%  29518   63   70  SE BREDBAND2 Bredband2 AB, Sweden
89.33%   3301  268  300  SE TELIANET-SWEDEN TeliaSonera AB, Sweden
```

Ranking only those ASs with more than 50 sample points in this experiment run (1014 AS's)

DNSSEC use in the RIPE Region...

Country Code	DNSSEC use	Clients who used DNSSEC Resolvers	Client count	
SE	62.74%	820	1307	Sweden
CZ	56.69%	1331	2348	Czech Rep.
SI	53.95%	839	1555	Slovenia
PS	53.79%	568	1056	Palestine
GL	53.33%	8	15	Greenland
AZ	49.93%	760	1522	Azerbaijan
LU	43.12%	138	320	Luxembourg
IE	41.22%	807	1958	Ireland
FI	37.60%	141	375	Finland
TR	34.82%	1793	5150	Turkey
TM	33.33%	1	3	Turkmenistan
KG	32.33%	43	133	Kyrgyzstan
BY	28.97%	352	1215	Belarus
IR	25.00%	1	4	Iran
IQ	23.43%	279	1191	Iraq
MT	22.59%	401	1775	Malta
LT	22.23%	623	2803	Lithuania
BA	21.78%	888	4077	Bosnia
TJ	18.75%	3	16	Tajikistan
UA	17.78%	1228	6906	Ukraine
AL	15.95%	107	671	Albania
SY	15.70%	27	172	Syria
PL	15.55%	1573	10115	Poland
LB	14.67%	71	484	Lebanon
NO	13.57%	267	1968	Norway
HU	12.68%	593	4675	Hungary
IT	12.45%	1217	9778	Italy
AM	11.14%	183	1642	Armenia
BH	10.34%	130	1257	Bahrain
KZ	10.18%	185	1818	Kazakhstan
SK	9.09%	117	1287	Slovakia
RO	8.68%	925	10658	Romania
DK	8.55%	118	1380	Denmark
EE	7.75%	41	529	Estonia
RU	7.59%	694	9149	Russia
BG	7.47%	716	9588	Bulgaria
AD	6.90%	2	29	Andorra
MC	6.67%	3	45	Monaco
MK	6.17%	43	697	Macedonia
IL	6.07%	176	2901	Israel
DE	6.00%	502	8371	Germany
IS	5.97%	12	201	Iceland
CH	5.95%	105	1765	Switzerland
LI	5.88%	1	17	Liechtenstein
LV	5.52%	47	852	Latvia
NL	5.36%	328	6119	Netherlands
MD	4.77%	101	2119	Moldova
YE	4.50%	42	934	Yemen
GI	3.70%	1	27	Gibraltar
UZ	3.68%	5	136	Uzbekistan
BE	3.11%	118	3794	Belgium
PT	2.71%	90	3323	Portugal
GB	2.66%	758	28453	UK
GE	2.45%	36	1472	Georgia
JO	2.36%	50	2118	Jordan
SA	2.33%	376	16169	Saudi Arabia
HR	2.30%	117	5077	Croatia
FR	2.30%	336	14625	France
AT	2.18%	177	8113	Austria
ES	2.15%	176	8168	Spain
OM	2.08%	36	1732	Oman
CY	2.03%	165	8137	Cyprus
GR	1.72%	562	32649	Greece
KW	1.70%	40	2359	Kuwait
AE	0.79%	114	14374	UAEs
QA	0.51%	37	7263	Qatar
SM	0.00%	0	6	San Marino
FO	0.00%	0	18	Faroe Islands

A Bit More...

1757200 tests performed over 12 days

15.70% = 275819

- this is the number of folk who pulled the crossdomain.xml, OR who pulled a result gif of zd-null.ze-null i.e. they retrieved NOTHING

8.17% = 143589

- this is the bunch of folk who pulled d.t5 and NOT e.t6 - i.e. potentially the number of IDs who did the first and NOT the seco

5.39% = 94655

- this is the number of clients who pulled the e.t6 and NOT the d.t5 - i.e. did the OPPOSITE

70.75% = 1243137 these folk pulled both.

A Bit More...

Hang on..

5% of the clients did the precise OPPOSITE of the “hints” provided by DNSSEC validation?

What are we observing in this experiment?

A Bit More...

The clients are browsers

- browsers look random:
  - browsers typically use a set of server ports and schedule tasks to ports
  - If a port has a large transfer underway subsequent tasks will block
  - Tasks passed to the browser from a script may be processed in a different order depending on other activity underway at the same time
- Browsers often are cut short
  - Users get bored
- Failure to fetch can happen for many reasons in a browser, only some of which may be DNSSEC invalidity

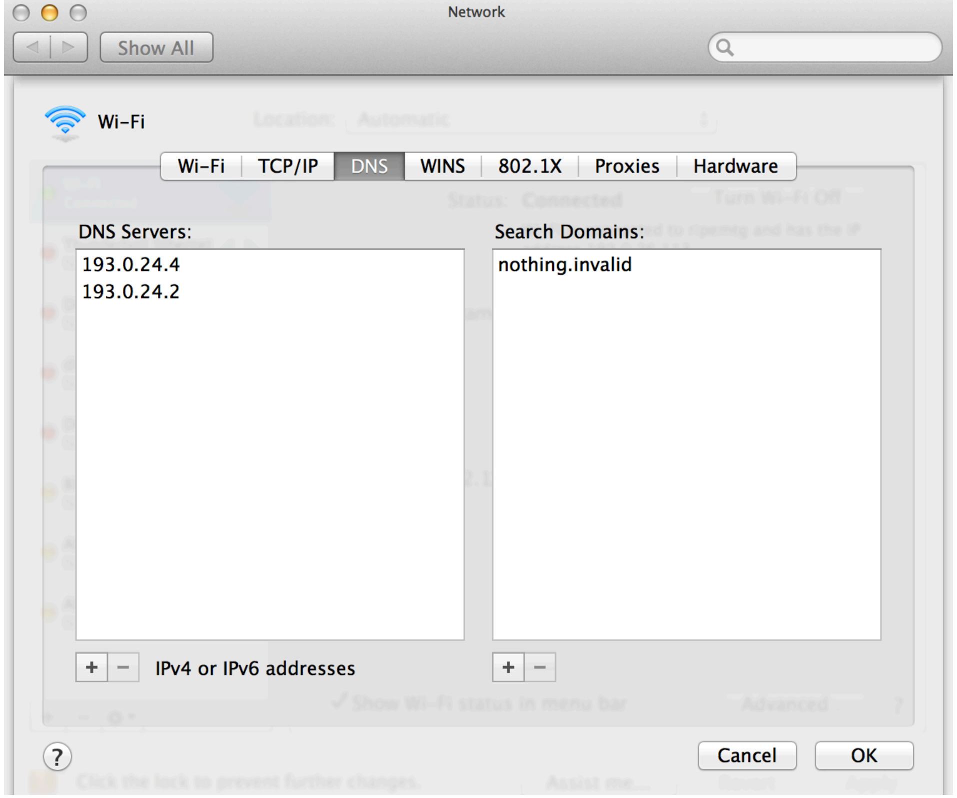
A Bit More...

Multiple Resolvers
It is not unusual to see service providers provide 2 (or even more) DNS resolver addresses to their clients

This allows for the situation when one server is unresponsive, borked or just having a bad hair day. The client is expected to query the other resolver in the resolver set

As well as timeout what other DNS responses will cause a client to query the other resolvers on the resolver list? SERVFAIL

What response will a DNSSEC-validating behaviour pass back to its client if DNSSEC validation fails?
SERVFAIL



DNS Servers:
193.0.24.4
193.0.24.2

Search Domains:
nothing.invalid

A Bit More...

How can we tell if a resolver performs DNSSEC validation?

We take as a strong clue that if the resolver retrieves DNSKEY RRs then it is performing DNSSEC validation

If the resolver also retrieves DS RRs then this supports that assumption

A Bit More...

How can we tell if a resolver is a DNSSEC-validating recursive resolver or a DNS forwarder?

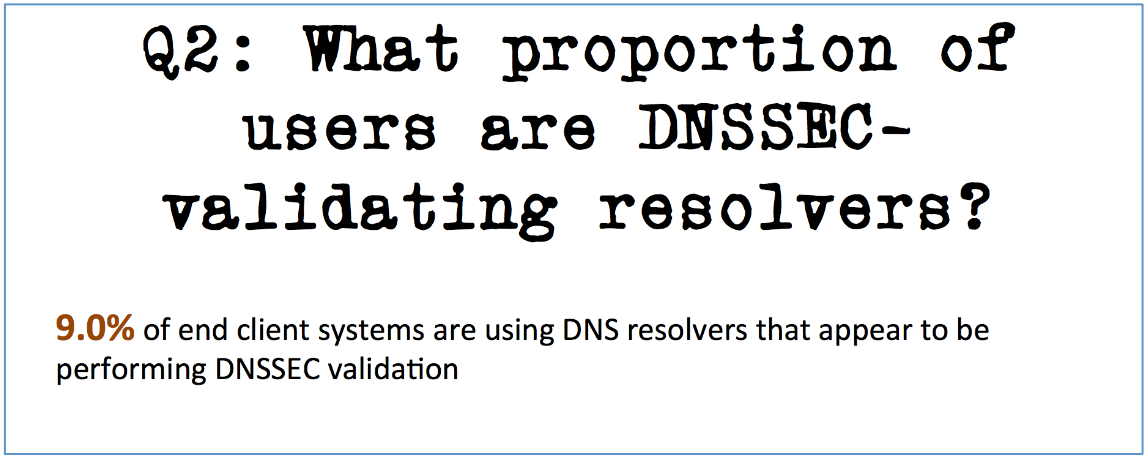
(“We” in this case is the authoritative name server)

Its not easy to tell the difference from this perspective

We have some theories that we’d like to try, but ideas are welcome

A Bit More...

So what does this mean?



Q2: What proportion of users are DNSSEC-validating resolvers?

9.0% of end client systems are using DNS resolvers that appear to be performing DNSSEC validation

It means that 9% of clients pass queries to DNS resolvers who, in turn perform DNSSEC Validation.

However we observe that, on average, clients generate queries that cause an average of 2.1 different resolvers to query our authoritative nameserver

And perhaps the most we can say is that

- A maximum of 9% of clients may not fetch an object that lies behind a DNSSEC-invalid validation chain
- But this is more like 4% **+/- 5%**, to be a little more overt about the uncertainties in this experiment

Resolver anomalies

8.8.8.8 anycast Public DNS

- 113 resolvers using Google’s IP space retrieved DNSKEY RRs
- 291 resolvers did not
- Drilling down
  - 25 routed prefix “sets” of resolvers
    - 15 of these resolver clusters did not retrieve DNSKEY RRs
    - 3 of these resolver clusters had resolvers that ALL retrieved DNSKEY RRs
    - 7 of these resolver clusters had mixed responses

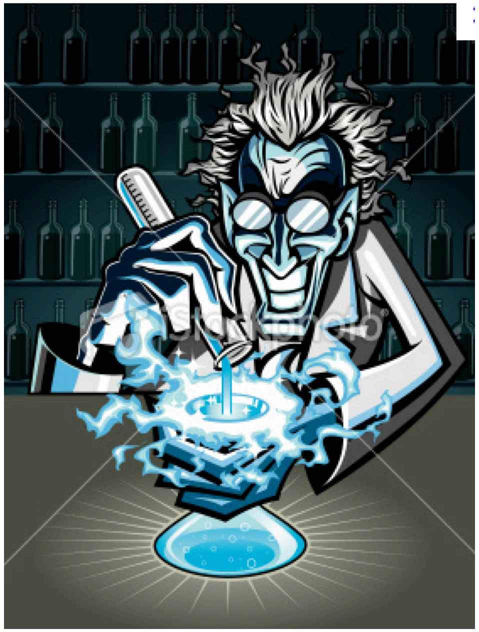
Resolver Anomalies

The "Mad Resolver" prize goes to the pair of resolvers:

217.73.15.39

217.73.15.38

who successfully queried for the same A RR from our server for a total of 93,237 times over eight hours



Thanks guys! Great achievement!

Thank you!

More details at: blabs.apnic.net