Number of possible DNSSEC validators seen at JP, 1 year difference

Kazunori Fujiwara, JPRS

<fujiwara@jprs.co.jp>

March 25, 2012

Contents

- Basic Idea: How to detect DNSSEC Validators
- JPRS' data
- Result from full packet capture
- Result from 2 of 7 JP DNS servers
- Conclusion

Basic Idea: How to detect validators

- JP DS RR has been introduced in root zone
- JP DNSKEY TTL is 86400, 1 day

- Thus, DNSSEC Validators send JP DNSKEY query once a day if the validators try to perform JP domain name validation everyday.

- Or, BIND 9 Validators seem to send JP sub-domain name DS queries for JP DNS servers.

Assumption

- Validators
  - – IP addresses which send JP DNSKEY queries (at JP DNS servers)
  - – Or, IP addresses which send JP sub-domain name DS queries (at JP DNS servers)
    - BIND 9 validators seem to send DS queries at zone cuts.
- Resolvers
  - – IP addresses which send JP zone queries (at JP DNS servers)

JPRS’ data sets

Overview of JP

- .JP has 1,264,331 registered domain names (Feb. 1, 2012)
- JP DNS servers serve 1.6 billion queries per day
- Collecting packet captures and query logs

Name	Operator	Location	Address (IPv4:7, IPv6:6, total 13)	Capture
A.DNS.JP	JPRS	JP*2	203.119.1.1, 2001:dc4::1	Pcap/Log
B.DNS.JP	JPNIC	JP*1	202.12.30.131, 2001:dc2::1	Pcap
C.DNS.JP	JPRS	Worldwide	156.154.100.5, 2001:502:ad09::5	Pcap
D.DNS.JP	IIJ	JP*2, US*2	210.138.175.244, 2001:240::53	Pcap
E.DNS.JP	WIDE	JP*1,US*1, FR*1	192.50.43.53, 2001:200:c000::35	Pcap
F.DNS.JP	NII	JP*1	150.100.6.8, 2001:2f8:0:100::153	Pcap
G.DNS.JP	JPRS	JP*1	203.119.40.1	Pcap/Log

JPRS’ data sets

- JPRS sometimes collects two days long full capture of DNS packets
  - Once a year: Same timing as DITL (at DNS-OARC)
  - When .JP was signed: 16 Oct. 2010
  - When JP’s DS RR was introduced into root zone: 4:38, Dec. 10, 2010 (UTC) before 6 hours and after 48 hours
  - World IPv6 day, 2011

- JPRS has been collecting DNS query log from 2 of 7 JP DNS servers for 8 years
  - Not all JP DNS servers
  - If number of DNSSEC Validators is calculated with the the querylogs, it outputs continuous information

Counting method

- Full packet capture
  - Excluded obviously different queries
  - Count number of IP addresses within each 24 hours
- Query log
  - Excluded obviously different queries
  - Treat an IP address is a validator if it sent JP DNSKEY queries in the past 7 days.
  - The data is used to extrapolate the result from packet capture

Presuming number of DNSSEC Validators from 2 of 7 DNS servers’ data

Number of queries that JPRS’ test Validator send to [AG].DNS.JP

```
20110210  JPquery=62  DNSKEYquery=0
20110211  JPquery=52  DNSKEYquery=1
20110212  JPquery=26  DNSKEYquery=1
20110213  JPquery=45  DNSKEYquery=0
20110214  JPquery=52  DNSKEYquery=0
20110215  JPquery=48  DNSKEYquery=0
20110216  JPquery=127  DNSKEYquery=0
20110217  JPquery=65  DNSKEYquery=0
20110218  JPquery=28  DNSKEYquery=0
20110219  JPquery=41  DNSKEYquery=1
20110220  JPquery=31  DNSKEYquery=1
20110221  JPquery=27  DNSKEYquery=0
20110222  JPquery=27  DNSKEYquery=0
20110223  JPquery=25  DNSKEYquery=0
20110224  JPquery=29  DNSKEYquery=1
```

- The Validator sends JP zone query everyday, then it sends JP DNSKEY query once a day.
- The Validator can choose 7 DNS servers, but we have only 2 servers’ LOG
- I made an assumption that Validators send JP DNSKEY queries to various DNS servers
- In the example, there are continuous 6 days that our query log cannot detect JP DNSKEY query from the server.
- Assumption: An IP address is a validator if it sent JP DNSKEY queries in the past 7 days.

  (call it as 1week extrapolation)

Result

Result of full packet capture (24hours)

Date	Begin Time UTC	Number of IP addresses			Number of queries	
		JP	DNSKEY	DS	DNSKEY	DS
2009/12/14	23:00	1738928	9	10	37	171
2010/4/13	15:00	1512338	10	7	42	13
2010/4/14	15:00	1504715	6	10	30	13
2010/10/16	15:00	1185367	745	57	2070	1108
2010/10/17	15:00	1523473	879	69	1561	2233
2010/12/10	5:00	1470601	2310	2432	5532	4867319
2010/12/11	5:00	1108265	2083	2296	6234	2335665
2011/4/12	12:00	1560468	3838	5979	27302	7326974
2011/4/13	12:00	1517979	3699	5826	26110	7295136
2011/6/7	11:00	1557000	4673	6925	34744	9990825
2011/6/8	11:00	1493595	4337	6875	38346	9295877
2011/12/13	0:00	1560377	7528	10046	51198	22308672
2011/12/14	0:00	1576341	7388	9998	50358	22602591

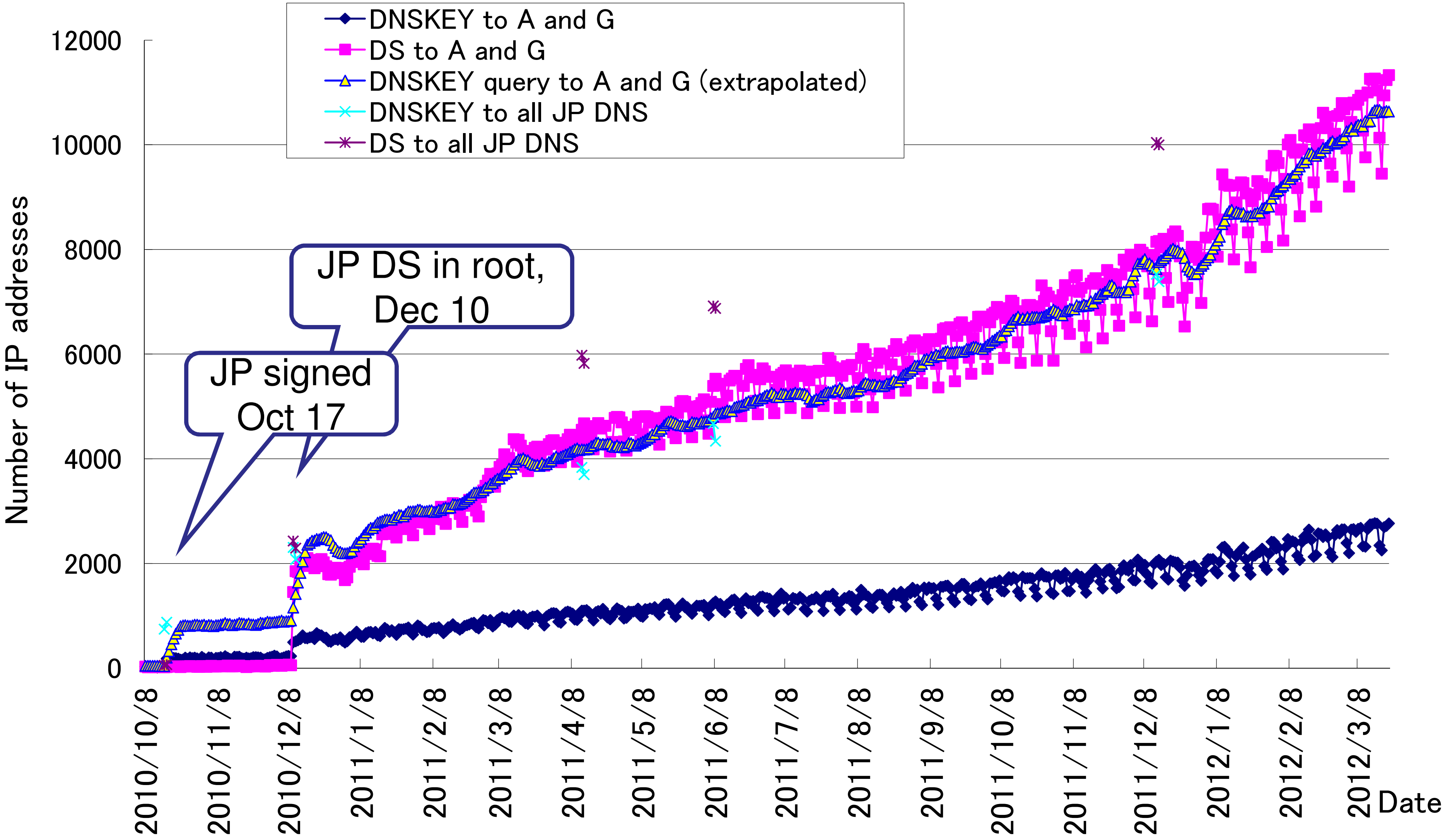
Result of full packet capture

- Number of IP addresses which sent JP DNSKEY queries was 7528, Dec 13, 2011
  - It increased by 5,000 IP addresses in one year
- Number of IP addresses which sent DS queries was 10,046, larger than number of IP addresses which sent JP DNSKEY queries
  - I don’t know why. Do you know?
  - About 1.5% of JP queries are DS, now
- Number of IP addresses which sent JP queries had not changed for a year.

Detailed analysis at Dec. 13, 2011

- Number of IP addresses which sent JP sub-domain name DS queries was 10046
  - Some IP addresses sent DS queries, but no DNSKEY queries: 3466
    - Did they make a DNSSEC validation ?
  - Some IP addresses sent DS query only: 320
    - Were they DNSSEC monitors ?
- Number of IP addresses which send JP DNSKEY queries was 7528, Dec 13, 2011
  - DNSKEY>0 and DS>0: 6557 … BIND 9?
    - But No other queries: 132 … tester?
  - DNSKEY>0 and DS=0: 961 … Unbound?
    - No other queries: 22 … monitor?

Number of possible DNSSEC Validators



JP DS in root, Dec 10

JP signed Oct 17

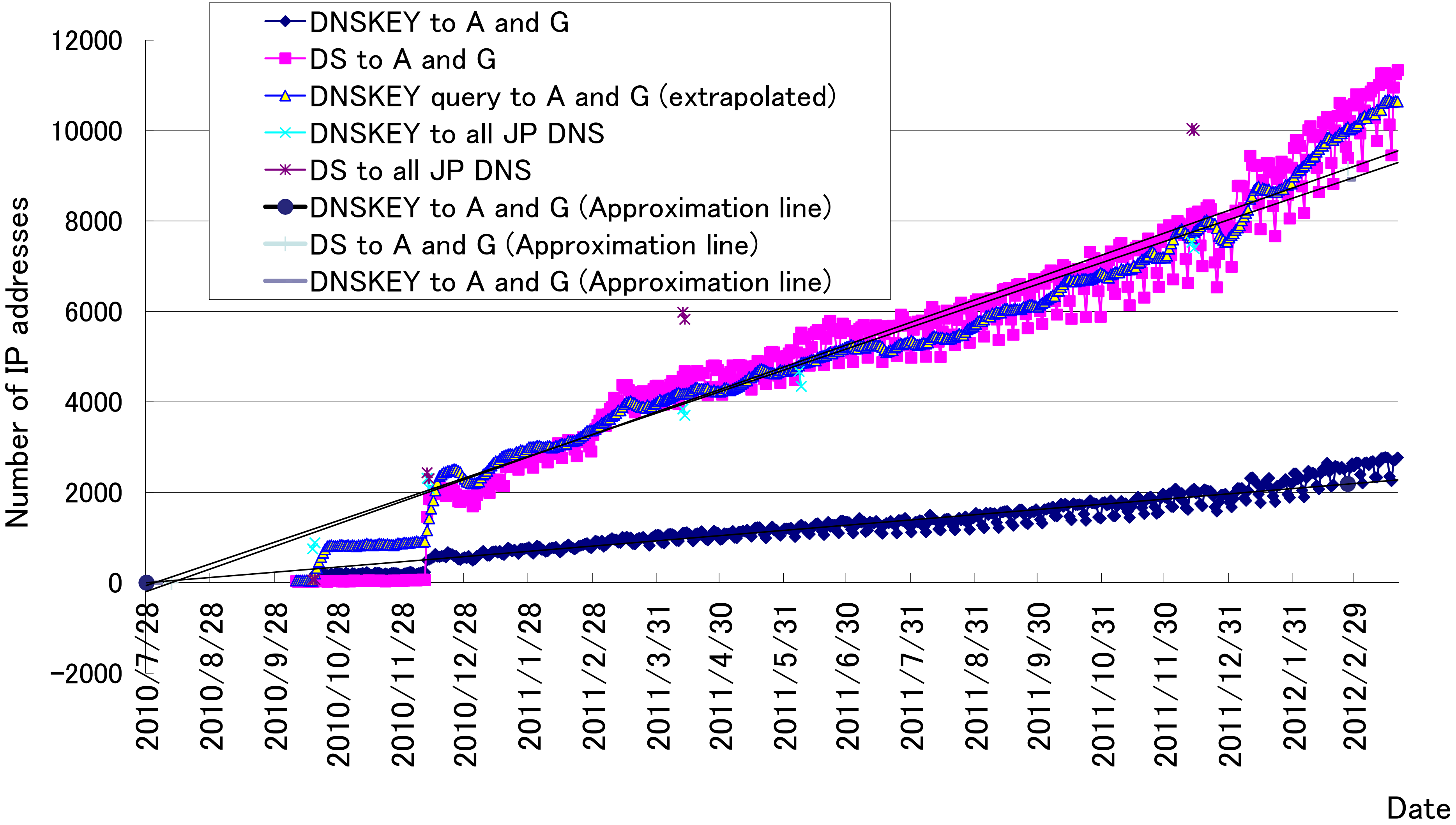
One year differences

- Number of IP addresses which send JP DNSKEY and *.JP DS is still increasing
  - About 10,000 hosts, (1 year ago, about 3,000)
  - Maybe linear, or higher
- Three numbers are almost the same
  - Presumed value of number of IP addresses which send JP DNSKEY queries for A and G
  - Number of IP addresses which send JP DNSKEY queries for all JP DNS servers
  - Number of IP addresses which send DS queries for A.DNS.JP and G.DNS.JP

approximated by the least square method

- After Dec 20, 2010 (10 days after JP DS in root)
- Number of IP addresses which send JP DNSKEY for A and G
  - 0.000043719 * t -55974 (t: unixtime)
  - Zero date = 1280316457, July 28, 2010
- Number of IP addresses which send DS queries for A and G
  - 0.000187344 * t -240046
  - Zero date = 1281311389, August 9, 2010
- Number of IP addresses which send JP DNSKEY for A and G, extrapolarated
  - 0.000179976 * t -230489
  - Zero date = 1280666979, August 1, 2010
  - The presuming technique delays 1 week. It may be July 25

Number of possible DNSSEC Validators with linear approximation



Result of the analysis

- We observed
  - – 3000 possible DNSSEC Validators in March 2011
  - – 10000 in Febrary 2012
  - – Number of Validators are still increasing
  - – The result of alignment approximation shows that number of DNSSEC validators is increasing linearly from the day when root was signed.
- The result may be larger than number of real DNSSEC Validators
  - – Because there may be many monitors, dig tests, …
  - – It shows people's interest
- Then, the result shows the number of DNSSEC Validators, and people's interest about DNSSEC Validation is still increasing linearly or higher.

Appendix

Exclusion

- If the IP address send
  - RD=1 (dig @server jp dnskey without +norecurse)
  - DO=0 (dig @server jp dnskey without +dnssec)
  - DNSKEY query only
    - (does not send normal JP queries)

queries, it is not a Validator.

about 10% of IP addresses send these queries