Number of DNSSEC validators seen at JP

Kazunori Fujiwara, JPRS

<fujiwara@jprs.co.jp>

March 27, 2011

IEPG

Contents

- Assumption
  - How to detect DNSSEC Validators
- JPRS' data
- Result from full packet capture
- Result from 2 of 7 JP DNS servers
- Conclusion and future works

- Differences from DNS-OARC presentation
  - Added March, 2011 data
  - Removed discussions about number of resolvers

Assumption

Assumption: 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.

Definition: Validators and Resolvers

- Validators
  - IP addresses which send JP DNSKEY queries (at JP DNS servers)
- Resolvers
  - IP addresses which send JP zone queries (at JP DNS servers)

Query ratio from DNSSEC Validators

- Number of queries from Validators =
  Number of queries originated by Validators

- Number of queries from all resolvers =
  Number of queries received by JP DNS servers

- Query ratio from DNSSEC Validatiors

=Number of queries from Validators /
Number of queries from all Resolvers

JPRS’ data sets

Overview of JP

- .JP has 1,207,100 registered domain names (March 1, 2011)
- 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	150.100.2.3, 2001:2f8:0:100::153	Pcap
G.DNS.JP	JPRS	JP*1	203.119.40.1	Pcap/Log

JPRS' data sets

- JPRS collected two days long full capture of DNS packets around JP DS was registered in root zone
  - JP's DS RR was introduced into root zone at about 4:38, Dec. 10, 2010 (UTC)
  - JPRS collected From 22:00 Dec. 9 to 14:00 Dec. 12, 2010 (UTC)
    - 6.5 hours before JP DS was introduced
    - 48.5 hours after JP DS was introduced
- JPRS has been collecting DNS querylog from 2 of 7 JP DNS servers for 7 years
  - A.DNS.JP and G.DNS.JP are operated by JPRS and located in Japan, easy to collect.
  - A.DNS.JP query log is collected for over 7 years
  - G.DNS.JP query log is collected for over 2 years

Result of full packet capture

When JP DS was introduced into root

- Two day (55 hours) total
  - 1,831,434 IP addresses send 3,709,177,100 JP queries
  - 3,315 IP addresses send 55,920 JP DNSKEY queries
  - 75% of DNSKEY queries came from one IP address
  - 5.6% of DNSKEY queries came from JPRS' monitors
- Calculated 4 time slot
  - Before JP DS was introduced: 6 hours
  - Changing 1 hour
  - First 24 hours after JP DS was introduced
  - Second 24 hours after JP DS was introduced

Result of 55 hours packet capture

	Total 55h	Before 6h	Changing 1h	First 24h	Second 24h
Begin Day/Time End Day/Time	9/22:00 12/04:00	9/22:00 10/04:00	10/04:00 10/05:00	10/05:00 11/05:00	11/05:00 12/05:00
Day of week	Fri-Sun	Friday	Friday	Fri-Sat	Sat-Sun
Num of Validators	3,315	280	118	2,468	2,277
Num of Resolvers	1,831,434	784,513	468,384	1,469,184	1,108,903
Ratio of Validators (%)				0.168 %	0.205 %
Num of query: from validators	220,000,744	1,014,282	477,893	83,947,487	65,179,656
Num of query: from resolvers	3,709,177,100	429,276,877	83,736,527	1,670,176,896	1,525,986,800
Validator's share of queries	5.93%	0.24%	0.57%	5.03%	4.27%

Date/Time is represented as UTC

Result of 2 of 7 JP DNS servers

Querylog from [AG].DNS.JP

- JPRS has been collecting querylogs from A.DNS.JP and G.DNS.JP for several years
  - Diffusion rate of DNSSEC Validation may be calculated from the querylogs
- But full-resolvers have cache function
  - JP DNSKEY TTL is 86400 (1 day)
  - Resolvers can choose 13 IP addresses
  - Then, JPRS' querylog does not contain full DNSKEY query
- How to adjust ?

DNSKEY queries from JPRS’ test Validator

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.
- 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.

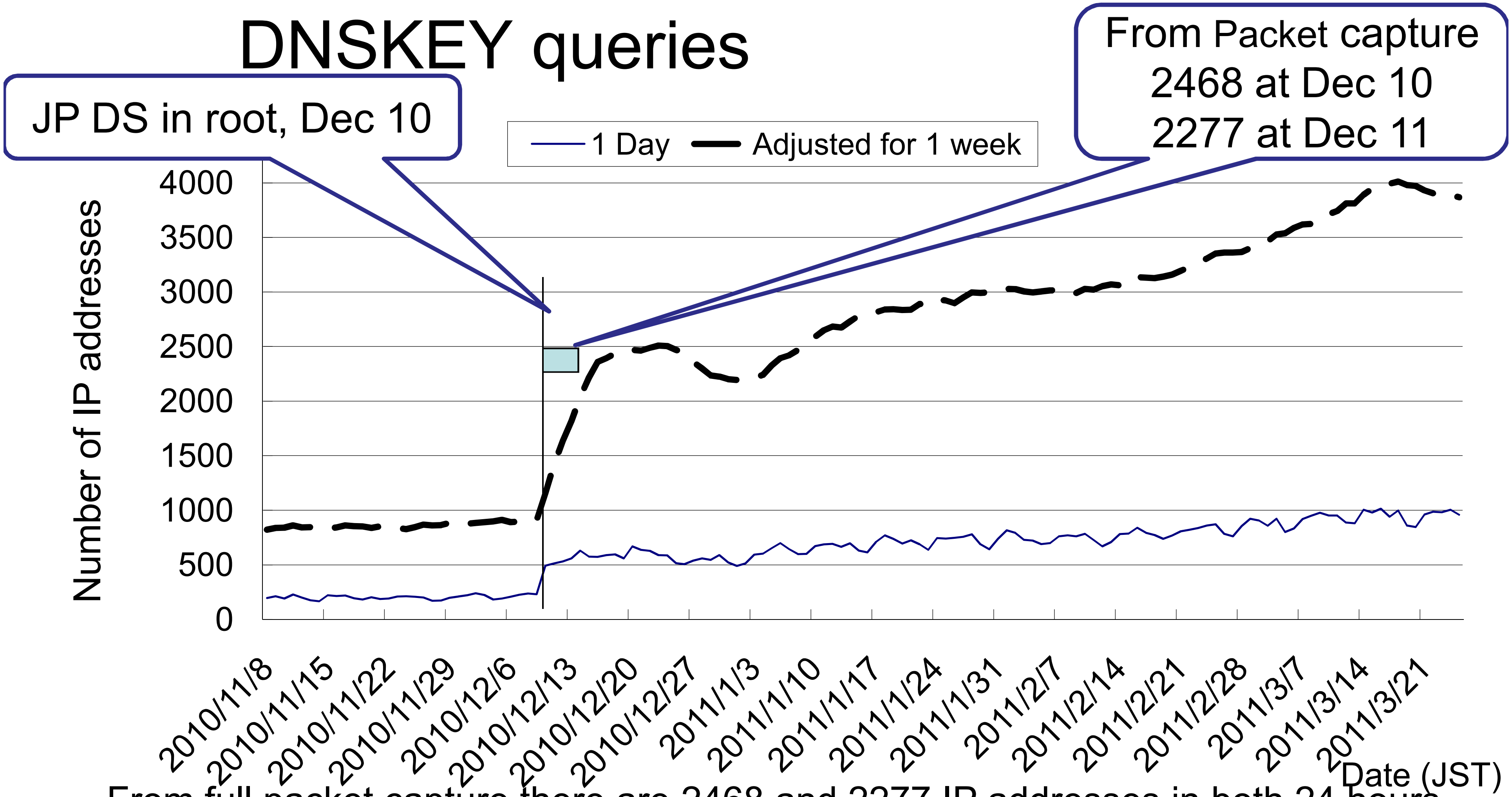
Exclusion

- 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.

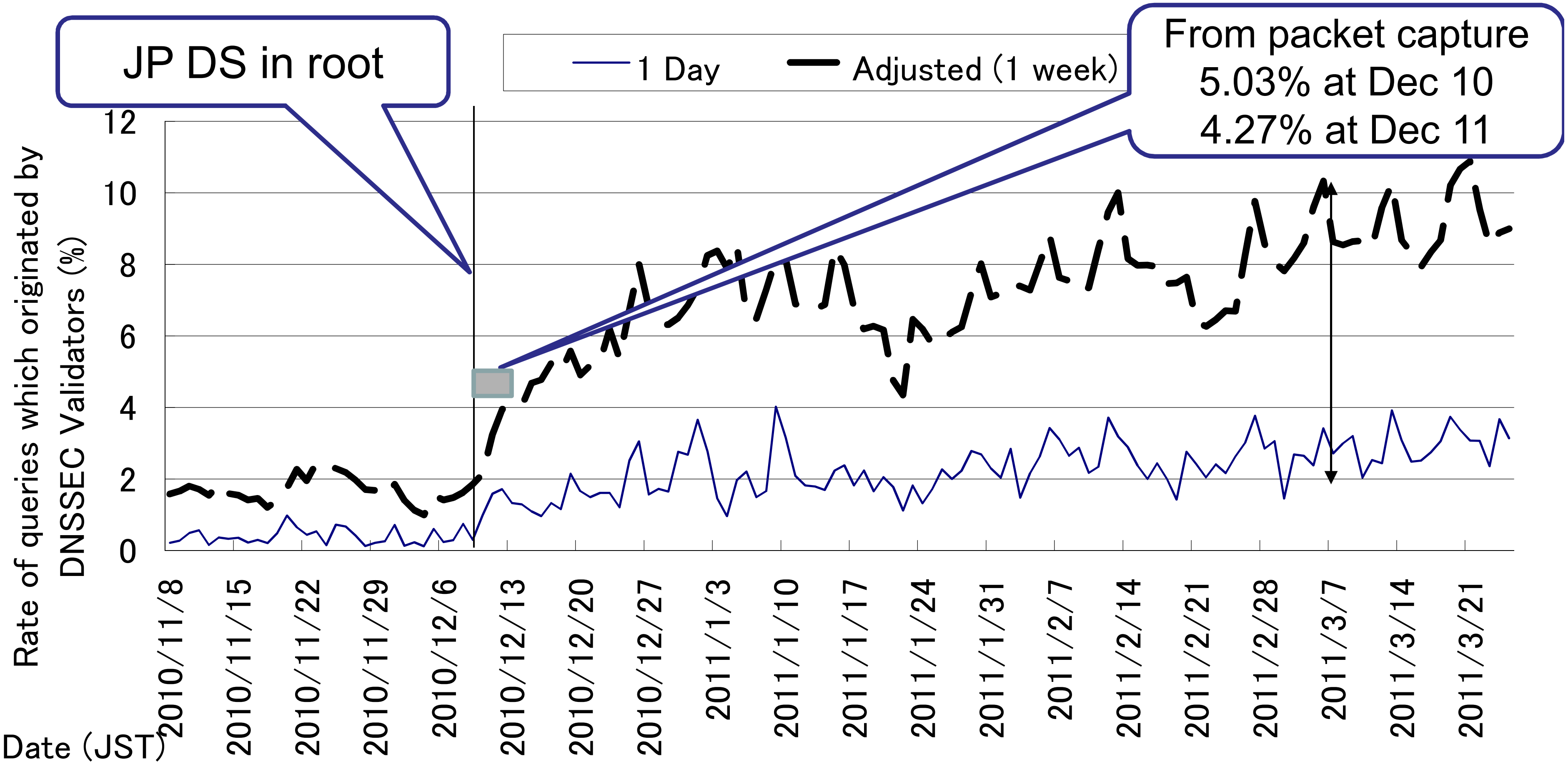
about 10% of IP addresses which send DNSKEY queries

Number of IP addresses which send JP DNSKEY queries



From full packet capture,there are 2468 and 2277 IP addresses in both 24 hours.
They are similar to the adjusted value 2400 at Dec 17 (7 days later from Dec 10).
The Adjustment seems to fit for DNSKEY query.

Query ratio from DNSSEC validators



2% of queries may come from DNSSEC monitors because it came before JP DS.
Increment is 7%. 7% of queries may come from DNSSEC validators

Cause of increase

- 7% of queries may came from Validators
- A large-scale organization might support DNSSEC validation.
- Or, some users of some large-scale organization send “JP DNSKEY” queries to their resolvers
  - It can not be identified ….

Who sent JP DNSKEY queries before JP DS was introduced in root

- About 900 IP addresses
- Why ?
  - There are many DNSSEC monitors
  - JPRS operates our service’s monitors
  - Someone set JP DNSKEY as a trust-anchor. (I did)
- IP addresses which send JP DNSKEY query before JP DS was introduced may not be real Validators.
- Then, the increment after JP DS introduction might be real DNSSEC Validators.
- There are 3,900 IP addresses which seems to send JP DNSKEY periodically
- Then number of real Validators are about 3,000

Conclusion and future works

Conclusion

- Tried to count DNSSEC Validators
- Number of Validators seems to be increasing
  - There seems to be about 3,000 Validators
  - They send 8% of queries
- Part of TLD DNS servers' querylog is useful to count number of DNSSEC validators

Future works and Questions

- Improving accuracy
  - More exclusion of DNSSEC monitors or users' interest
- More data
  - DNS-OARC has root capture data
  - Let's evaluate number of DNSSEC Validators
- Comments & Questions ?