Number of DNSSEC validators seen at JP

Kazunori Fujiwara, JPRS
<fujiwara@jprs.co.jp>

14 June, 2011

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.

Assumption

- 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 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 sometimes collects two days long full capture of DNS packets
  - Once a year, 50 hours: 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

- JPRS has been collecting DNS query log from 2 of 7 JP DNS servers for 7 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

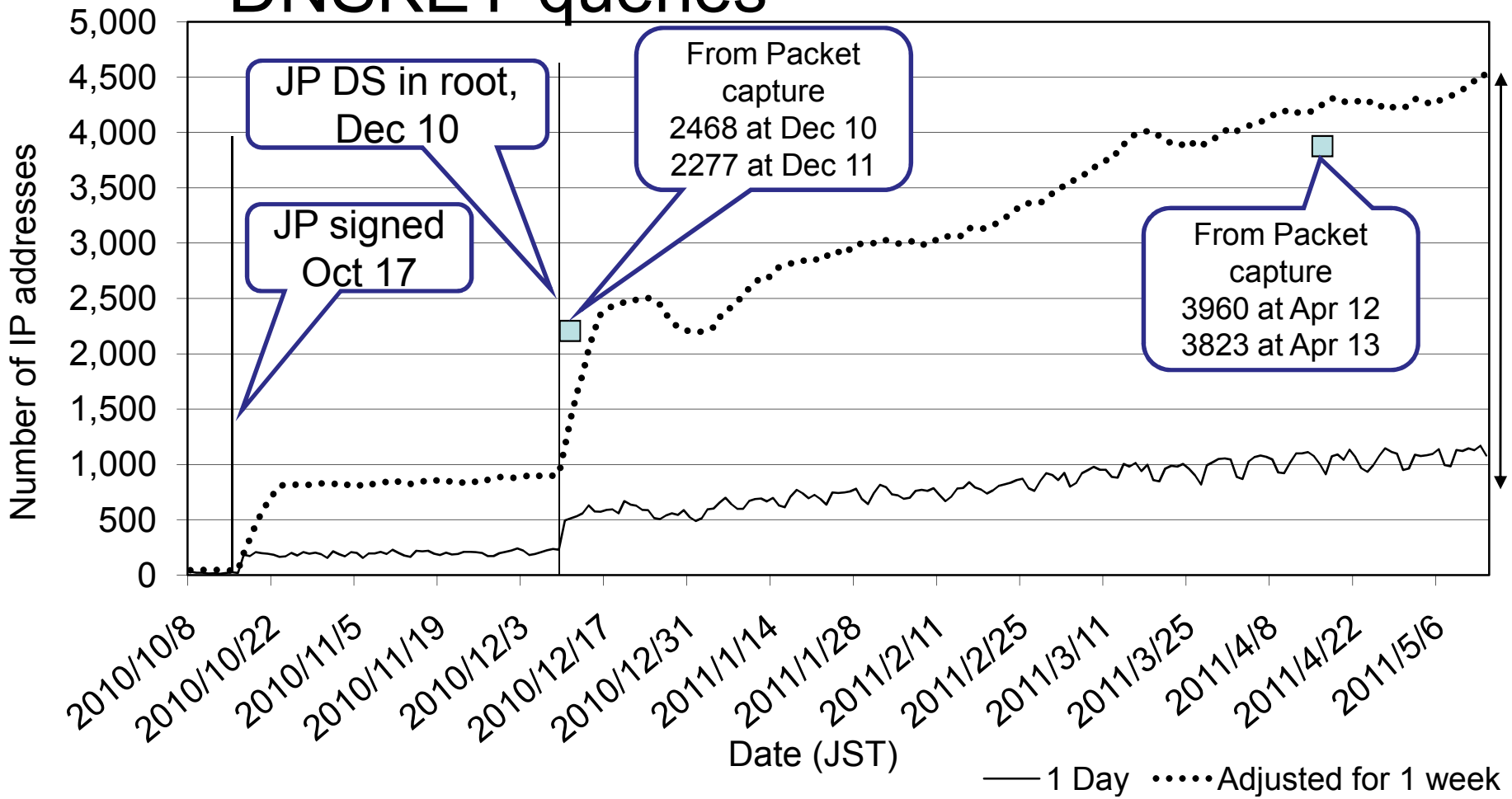
Result

Result of full packet capture

	2011/12/09 Before 6h	2011/12/10 24h	2011/12/11 24h	2011/4/12 24h	2011/4/13 24h
Begin Day/Time End Day/Time	9/22:00 10/04:00	10/05:00 11/05:00	11/05:00 12/05:00	12/12:00 13/12:00	13/12:00 14/12:00
Day of week	Friday	Fri-Sat	Sat-Sun	Mon-Tue	Tue-Wed
Num of Validators	280	2,468	2,277	3,960	3,823
Num of Resolvers	784,513	1,469,184	1,108,903	1,560,993	1,509,963
Ratio of Validators (%)		0.168%	0.205%	0.253%	0.253%
Num of query: from validators	1,014,282	83,947,487	65,179,656	78,098,447	70,418,839
Num of query: from resolvers	429,276,877	1,670,176,896	1,525,986,800	1,351,263,149	1,386,483,446
Validator's share of queries	0.24%	5.03%	4.27%	5.78%	5.08%

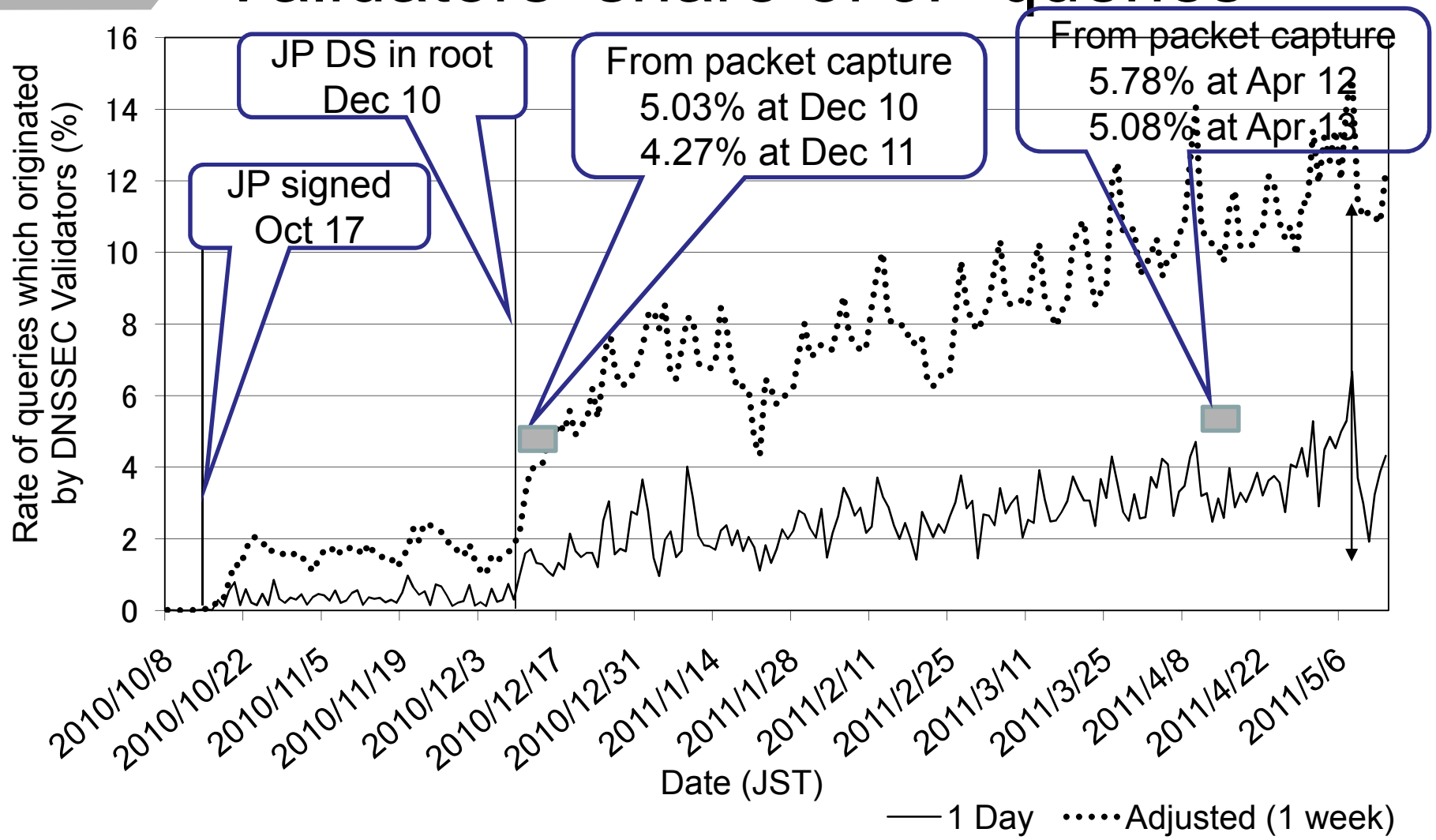
Date/Time is represented as UTC

Number of IP addresses which send JP DNSKEY queries



About 900 IP addresses send JP DNSKEY queries before JP DS was in root.
They may be DNSSEC monitors.
Increment before Dec. 10 and now is about 3600. There may be 3600 Validators.

Validators' share of JP queries



2% of queries may come from DNSSEC monitors because it came before JP DS.
1-week adjustment does not fit for this analysis.

Result of the analysis

- We observed
  - Hundreds of IP addresses started sending periodic JP DNSKEY queries immediately after JP was signed
  - 3600 DNSSEC Validators in May 2011
  - Number of Validators are still increasing
  - Validators send 5% or 10% of DNS queries
- The result may be larger than number of REAL DNSSEC Validators
  - If some users of a large-scale organization send “JP DNSKEY” queries to their resolvers, the resolver send “JP DNSKEY” query to JP DNS and the resolver is treated as DNSSEC Validator
  - It cannot be distinguished from REAL DNSSEC Validator

Conclusion

- Anyone can count number of DNSSEC Validators
  - if your zone is signed
  - and you capture your DNS server's query

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

Adjustment for 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
- 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 adjustment)