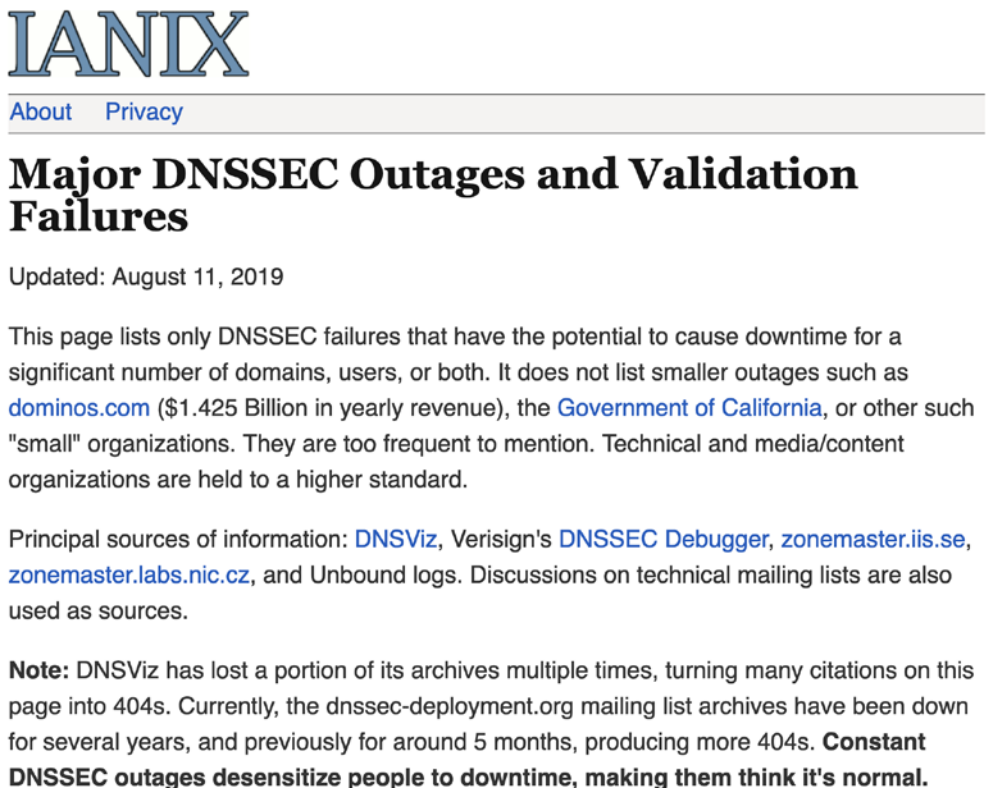
Towards detecting DNSSEC validation failure with passive measurements at TLD DNS servers

Kensuke Fukuda (NII)
Yoshiro Yoneya (JPRS)
Takeshi Mitamura (JPRS)

ICANN DNSSEC and Security Workshop
Nov 6, 2019

Introduction

- DNSSEC validation failure happens frequently
- Reliability of operation is a key of deployment



IANIX

About Privacy

Major DNSSEC Outages and Validation Failures

Updated: August 11, 2019

This page lists only DNSSEC failures that have the potential to cause downtime for a significant number of domains, users, or both. It does not list smaller outages such as dominos.com ($1.425 Billion in yearly revenue), the Government of California, or other such "small" organizations. They are too frequent to mention. Technical and media/content organizations are held to a higher standard.

Principal sources of information: DNSViz, Verisign's DNSSEC Debugger, zonemaster.iis.se, zonemaster.labs.nic.cz, and Unbound logs. Discussions on technical mailing lists are also used as sources.

Note: DNSViz has lost a portion of its archives multiple times, turning many citations on this page into 404s. Currently, the dnssec-deployment.org mailing list archives have been down for several years, and previously for around 5 months, producing more 404s. **Constant DNSSEC outages desensitize people to downtime, making them think it's normal.**

Research question

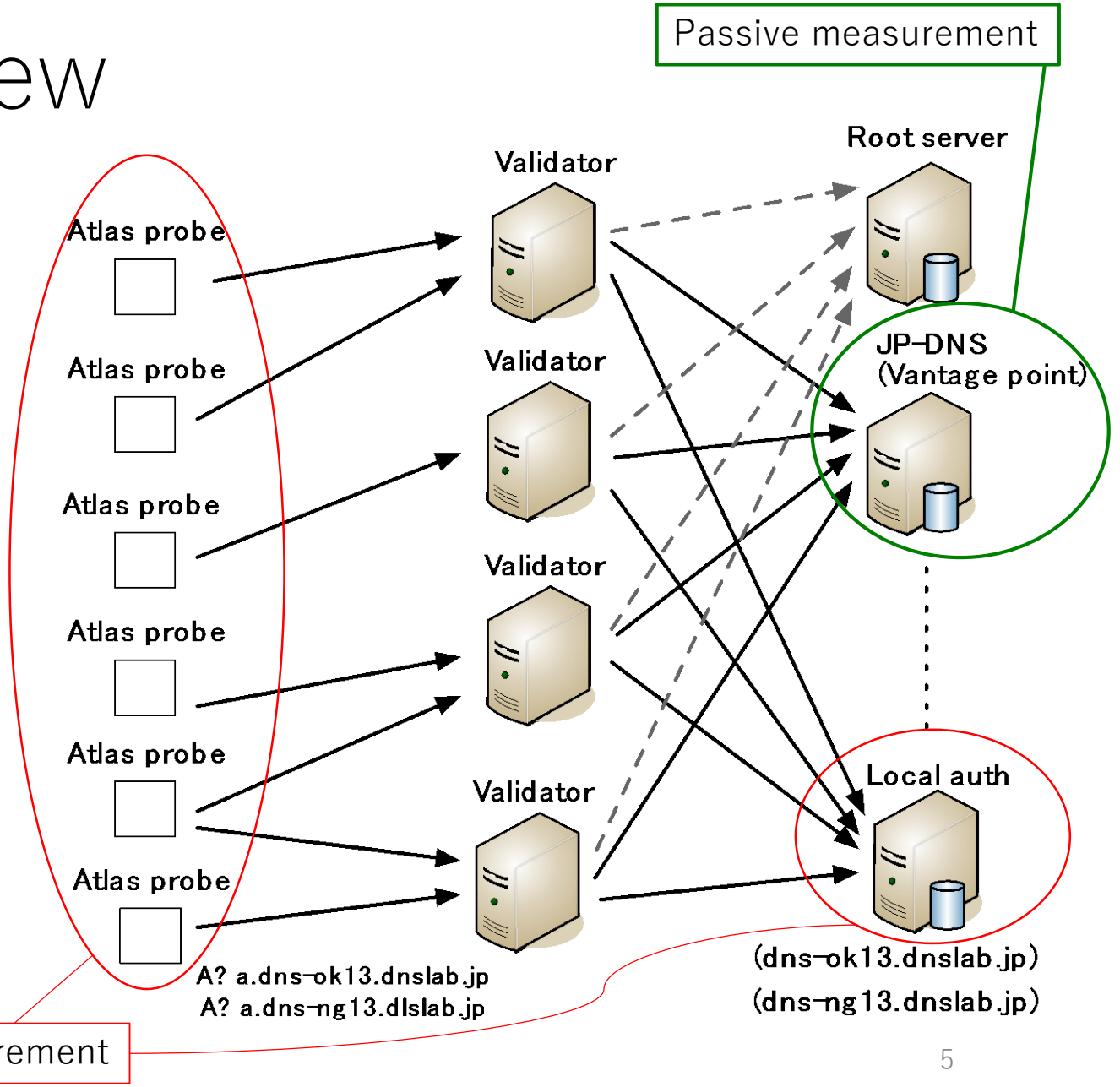
- How to detect validation failure rapidly and efficiently?
  - Active measurement
    - Periodic querying to authoritative servers
    - Higher loads for more DNSSEC available domains
  - Passive measurement
    - Change of query patterns could be a good indicator?

Towards detecting validation failures with passive measurements

- Goal:
  - Detecting change of query patterns at ccTLD servers before and after failure
- Current our work: Analysis with active measurements
  - DNS clients:
    - RIPE Atlas probe
    - DNSSEC validators (approx. 500) at ISPs or edges (not public DNS)
  - Local authoritative DNS server (3LD):
    - Successful and failed validator settings
    - Different TTL settings
  - Vantage point:
    - JP-DNS (ccTLD of JP)

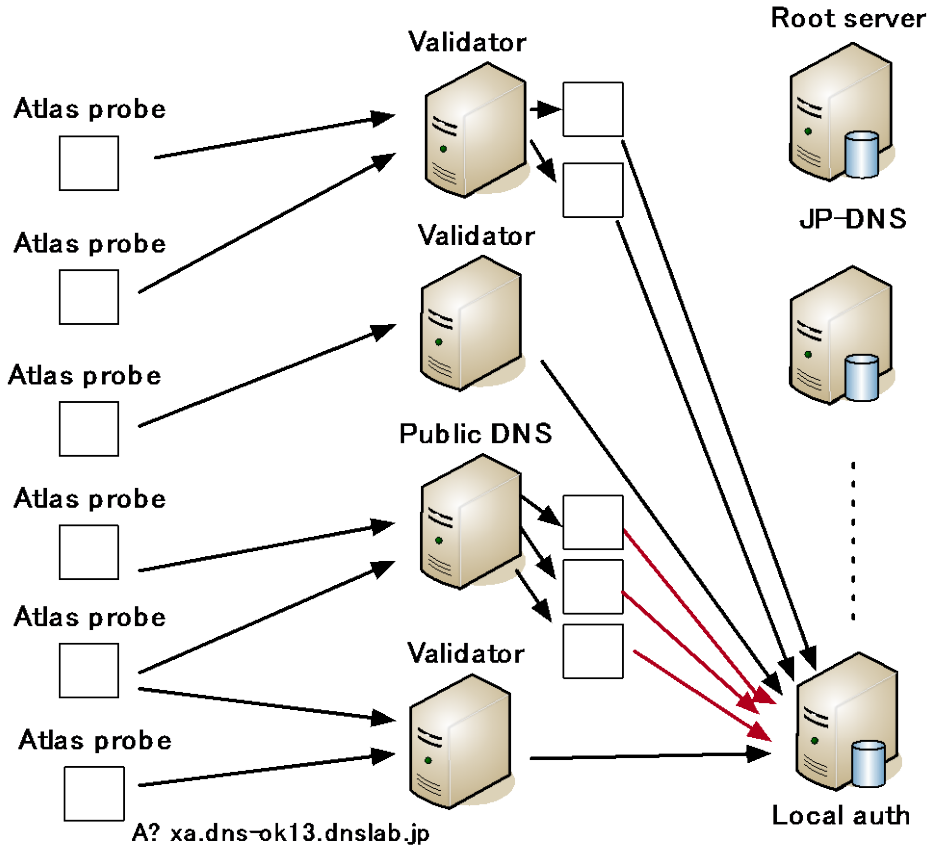
Measurement overview

- Measurement period
  - Apr 2018 (50hrs)
- Vantage point:
  - ccTLD (JP)
- Local authoritative:
  - 3LD (e.g. a.dns-ok13.dnslab.jp)
- Target queries
  - NS, A, DNSKEY, NS
- RIPE atlas probes
  - 600 DNSSEC validators at home



How to find non-public DNSSEC validators

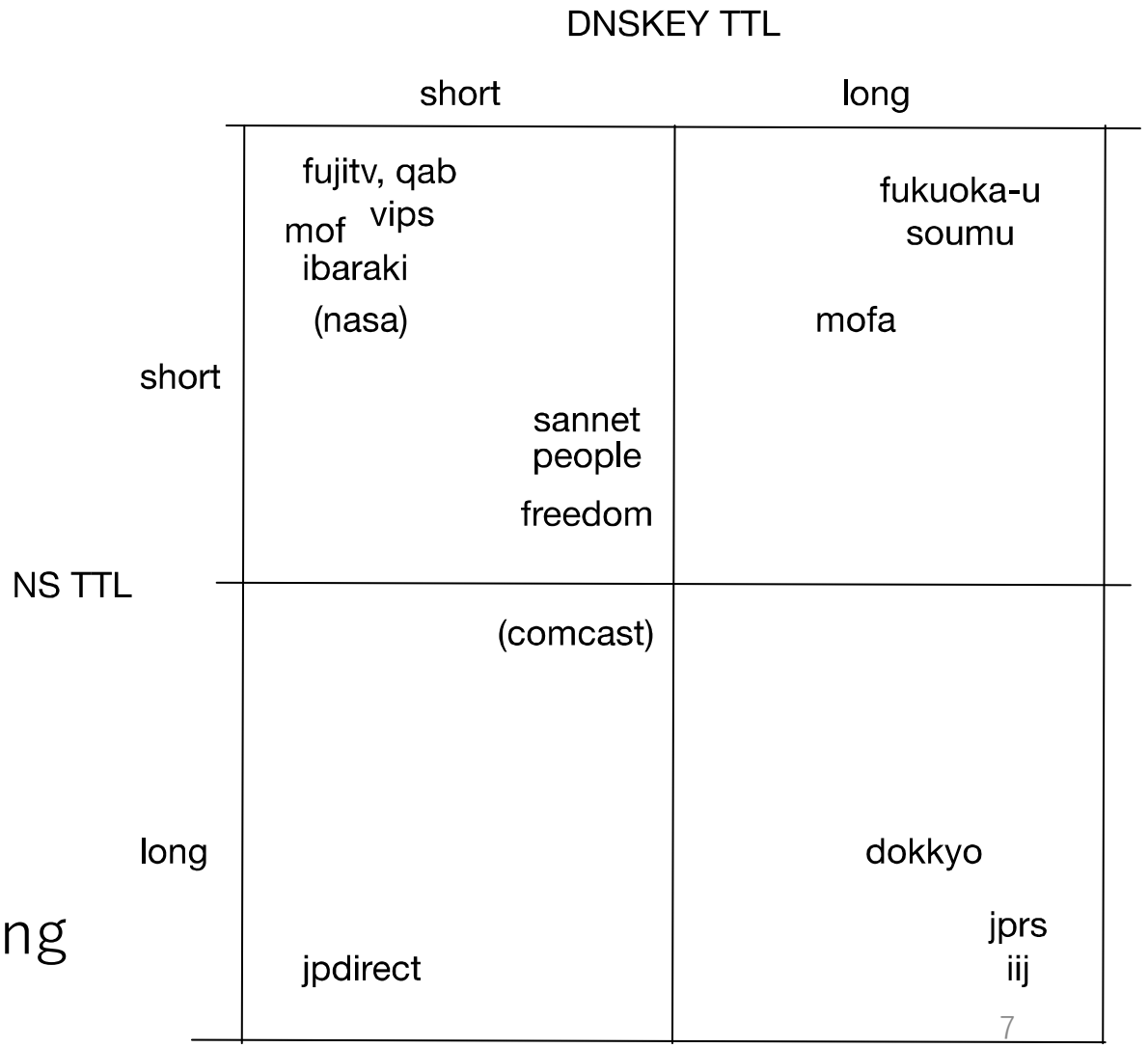
- Matching RIPE atlas probe logs to local auth logs
  - Atlas probe with home and stable-1day tags
  - Send unique A query (prepended timestamp and probe ID) with DO
  - Check query's src IP at local auth
    - E.g., ignore probes if corresponding src IPs belong to google
  - Check reply's AD flag
  - Use 602 probes and 985 resolvers



TTL parameters in JP DNSSEC domains

- NS and TTL settings
  - NS short and DNSKEY short
    - Media sites
  - NS long and DNSKEY long
    - ISP, registry
  - NS middle and DNSKEY middle
    - ISPs
  - NS short and DNSKEY long
    - government

No clear recommendations on each setting



Parameter settings

Name	Valid	TTL				Interval	Duration
		NS	DKEY	DS	A		
ok13	y	600	600	7200	600	540	8100
ok23	y	600	7200	7200	600	540	8100
ok33	y	7200	600	7200	600	540	8100
ok43	y	7200	7200	7200	600	540	8100
ng13	n	600	600	7200	600	540	8100
ng23	n	600	7200	7200	600	540	8100
ng33	n	7200	600	7200	600	540	8100
ng43	n	7200	7200	7200	600	540	8100

- Valid: successful validator (y) and failed validator (n)
- Interval: query interval from each probe
- Duration: measurement period for each probe

Parameter settings

DS and A are fixed
Interval and duration are also fixed

Successful validators

Failed validators

Name	Valid	TTL				Interval	Duration
		NS	DKEY	DS	A		
ok13	y	600	600	7200	600	540	8100
ok23	y	600	7200	7200	600	540	8100
ok33	y	7200	600	7200	600	540	8100
ok43	y	7200	7200	7200	600	540	8100
ng13	n	600	600	7200	600	540	8100
ng23	n	600	7200	7200	600	540	8100
ng33	n	7200	600	7200	600	540	8100
ng43	n	7200	7200	7200	600	540	8100

- Valid: successful validator (y) and failed validator (n)
- Interval: query interval from each probe
- Duration: measurement period for each probe

Results: Queries at local authoritative

name	All	A	DKEY	DS	NS
ok13	16003	6777	5512	2705	745
ok23	12938	6973	2117	2834	767
ok33	16018	6841	5675	2858	370
ok43	11424	6469	2003	2622	188

Successful

name	All	A	DKEY	DS	NS
ng13	64439	14929	38319	7781	2688
ng23	63847	15292	37017	8012	2743
ng33	62805	14661	37161	7841	2397
ng43	61283	14755	35488	7785	2471

Failed

- Overall queries increased in failure (as expected)
  - Due to negative cache
  - All 5x, A 2x, DKEY 7x, DS 3x, NS 6x
- TTL settings for NS and DNSKEY worked in successful validator

Queries at ccTLD (JP-DNS)

name	All	A	DKEY	DS	NS
ok13	1456	1305	61	87	2
ok23	1816	1705	14	91	1
ok33	1415	1268	39	101	0
ok43	1285	1171	12	99	0

Successful

name	All	A	DKEY	DS	NS
ng13	2342	2081	136	114	1
ng23	1958	1777	71	105	1
ng33	1594	1372	105	110	1
ng43	1468	1279	81	104	1

Failed

- Still queries increased, but not so significant
  - DNSKEY is a better indicator than DS
  - Longer DNSKEY TTL is better (due to negative cache?)

Queries at ccTLD (JP-DNS)

name	All	A	DKEY	DS	NS
ok13	1456	1305	61	87	2
ok23	1816	1705	14	91	1
ok33	1415	1268	39	101	0
ok43	1285	1171	12	99	0

Successful

name	All	A	DKEY	DS	NS
ng13	2342	2081	136	114	1
ng23	1958	1777	71	105	1
ng33	1594	1372	105	110	1
ng43	1468	1279	81	104	1

Failed

- Still queries increased, but not so significant
  - DNSKEY is a better indicator than DS
  - Longer DNSKEY TTL is better (due to negative cache?)

Attenuation at ccTLD

name	All	A	DKEY	DS	NS
ng13	64439	14929	38319	7781	2688
ng23	63847	15292	37017	8012	2743
ng33	62805	14661	37161	7841	2397
ng43	61283	14755	35488	7785	2471

Local authoritative

name	All	A	DKEY	DS	NS
ng13	2342	2081	136	114	1
ng23	1958	1777	71	105	1
ng33	1594	1372	105	110	1
ng43	1468	1279	81	104	1

ccTLD (JP-DNS)

- Huge attenuation of observable queries
  - All 30x, A 7x, DNSKEY 300x, DS 200x
- A validation failure in minor domains is likely difficult to detect

Conclusion

- We conducted DNS passive and active measurement to know query behaviors in DNSSEC failure
  - Active: RIPE Atlas probes
  - Passive: ccTLD (jp) and local authoritative
- DNS queries increased at DNSSEC validation failure
  - Attenuation of queries in DNS hierarchy
  - DNSKEY difference is still a good metric to detect validation failure
  - DS is not so significant

Future work

- Further large-scale studies required
  - Difference in public and other resolvers
  - Quantify ccTLD, 2LD, and 3LD attenuation
  - TTL effects in failure
  - Longitudinal analysis of a part of JP-DNS servers' traces
  - Effective (quasi-)realtime detection method at TLD servers' side