Zone monitoring for incremental DNSSEC adoption on critical TLD DNS

2012.10.14

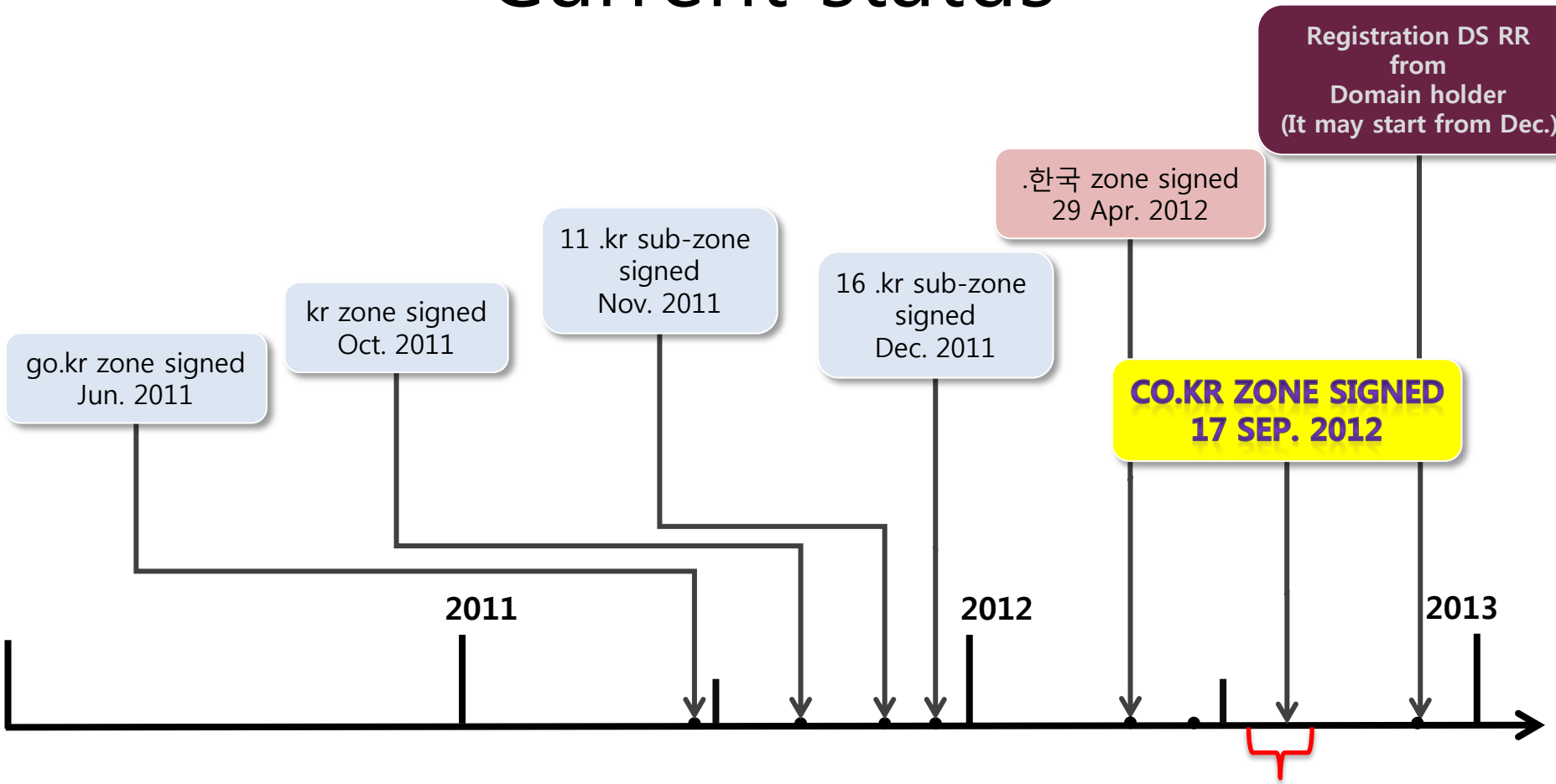
DNS-OARC Workshop, Toronto

Joonhyung Lim, Associate Research Fellow (jhlim@kisa.or.kr)
Han Sang Lee, Senior Research Associate (leehs@kisa.or.kr)

Korea Internet & Security Agency(KISA)

.KRNIC
KISA
한국인터넷진흥원

Current status



- 30 sub-domain zone under .kr ccTLD zone
- 1 multi-lingual domain zone ".한국"

DS RR added on Root DNS

- .kr zone : 201110
- .한국 zone2012,6

Before one step forward…

- 30 out of 31 zones we have signed for a year step by step.
- However, almost 80% of domain names served under “co.kr” zone.

- Hypothesis : If we sign, lots of NSEC RR will published to all over resolvers for every single query.
  - Just because we don’t have lots of DS RR in domain zone yet.
  - So, it makes more DNS traffic ever than before.
  - Also, it needs more memory for caching ever than before.

What we worried about…

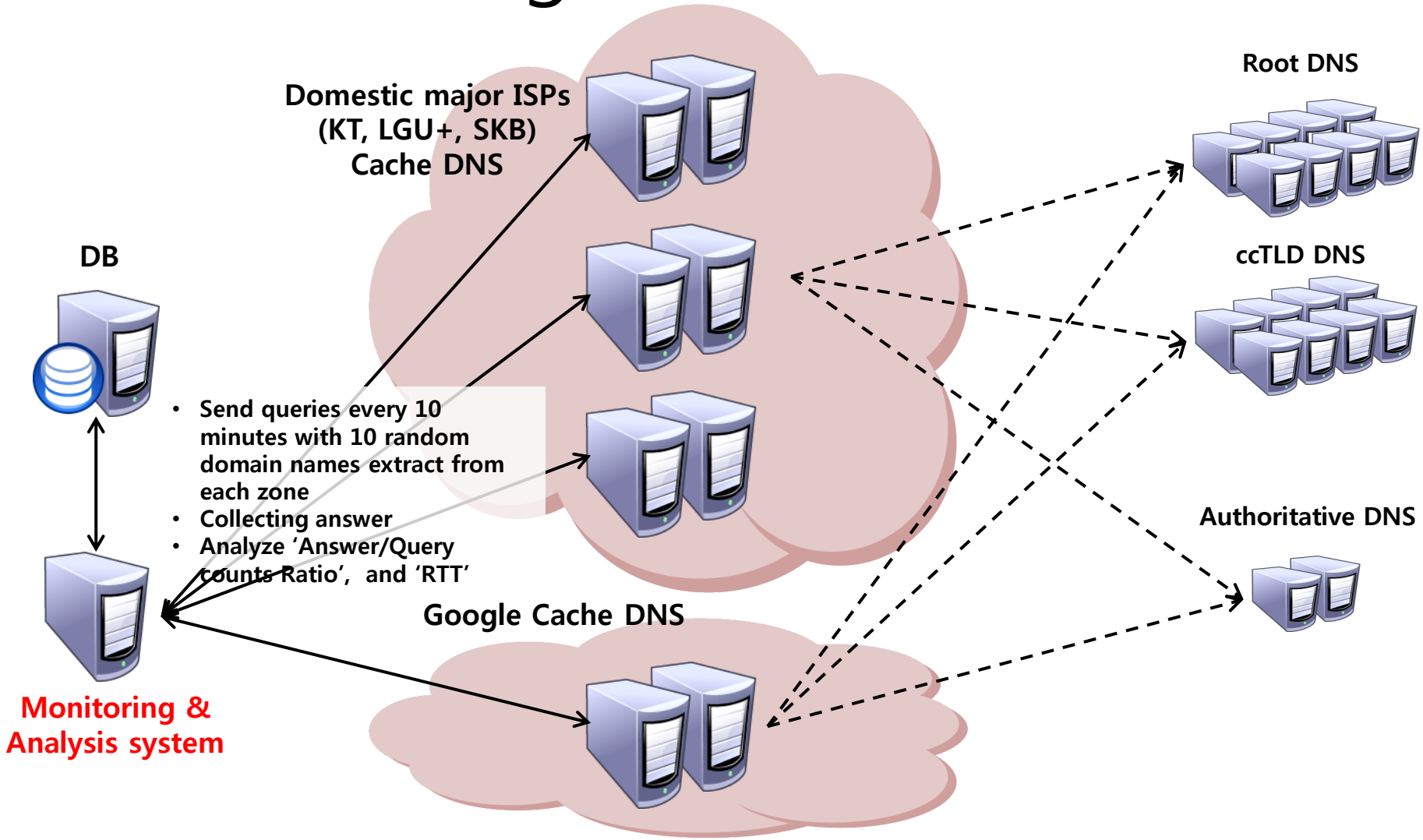
- Performance of our auth DNS
  - Some old servers may not serve zones very well.
  - Some servers connected to low-bandwidth upstream network may saturated due to a big answer packets.

- End-user influence triggered by what we did.
  - Most of domestic users are leashed by big cache DNS under 3 dominant ISPs.
  - Every wired or wireless devices(incl. cellular data) start communication with DNS queries.
  - So, if big cache is in trouble, users also will be in trouble.

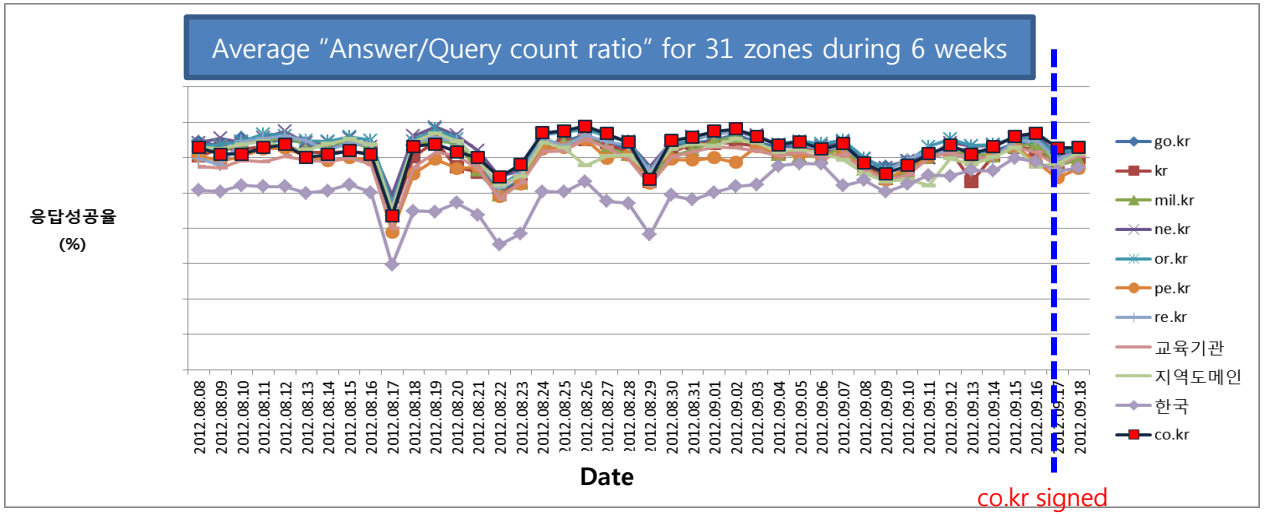
Question

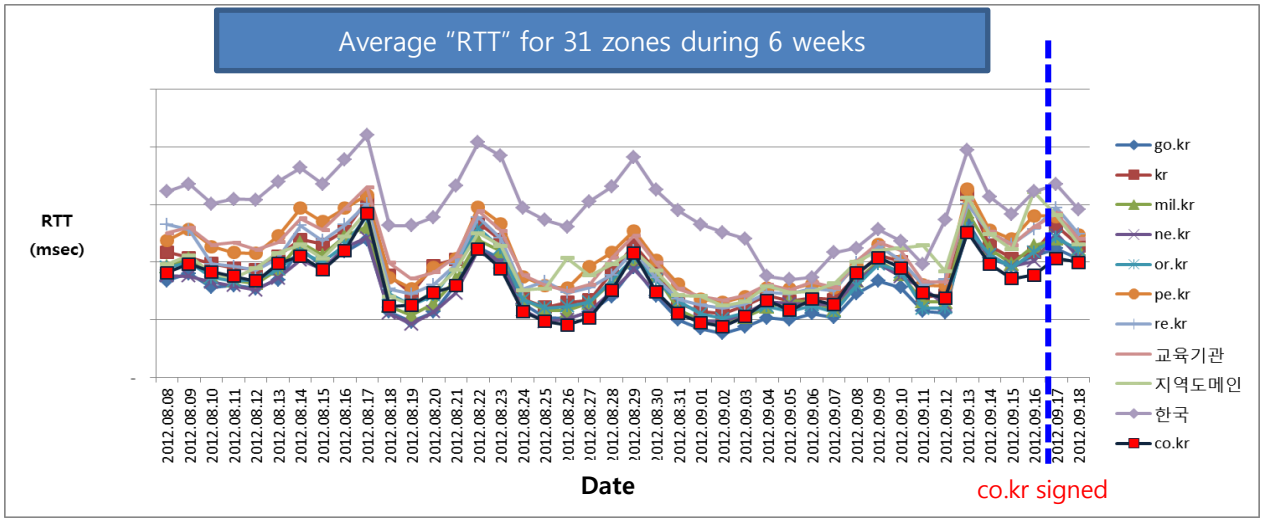
- Can we noticed differences on end-user side between before and after signing co.kr zone?
  - What we want to know is, whether a end-user takes more time for getting answer from massively big sign ed zone.
  - Enough measured data need to be collected from close to user-side for comparing with after signed.
  - Through comparing data, we might easily notice if something happens right after signed.

How to gather initial data



What we got


Average "Answer/Query count ratio" for 31 zones during 6 weeks
응답성공율
(%)
Date
co.kr signed
go.kr
kr
mil.kr
ne.kr
or.kr
pe.kr
re.kr
교육기관
지역도메인
한국
co.kr


Average "RTT" for 31 zones during 6 weeks
RTT
(msec)
Date
co.kr signed
go.kr
kr
mil.kr
ne.kr
or.kr
pe.kr
re.kr
교육기관
지역도메인
한국
co.kr

What we learned

- Some limitation comes from:
  - Upstream provider
  - Unnoticeable maintenance on DNS
- Each measured data is not say anything.
  - Only “average” between certain period is meaningful .
  - At a glance, we can easily see which zone need to be tuned against others.
- At least, from now, we can get alarm if something happens near major cache DNS, or each zone.

What's on next?

- We'll cooperate with ISPs to expand monitor coverage for focusing on their end-users.
- We'll make continuing efforts to raise awareness for domain holders and DNS providers.
- We'll also try to lots of talk with DNS community.

Thanks!

If you have question,

Email : jhlim@kisa.or.kr

Twitter: @_vasily