Time to stride towards differentiating DNS services?

Dr. Xiaodong Lee

OARC 2010 autumn, Denver
Domain Names in CN

Query_count_in_24_hour > 10 ? active : inactive
Cumulative Distribution of Query Load

80% queries are absorbed by 0.6% domains
Validity of Queries for CN Domains (2009/8/16)

52.8% queries are spam related.
We can see

Domains are not only literally different, some of them are:

- sleeping
- quite active
- financial related
- owned by big companies
- owned by criminals
Can we ...

Because the resolving capacity is limited, to make the usage of the resource more efficiently, can we

Provide service for domains in different levels?
Measures we are taking now

- Registry side
  - Registration information validation
  - Phishing check
  - Domain owner reputation database

- Operation side for VIP domains
  - Strict DNS update checking
  - Query amount monitoring
  - Real time query result monitoring
But we still can not

- Intelligently block bad domains.
- Guarantee QoS for important domains.
- Balance the cost and service quality in quantitative measurement
Proposal--Domain Ranking System
( NOTE: very fresh idea)

- Each domain is assigned a value.
- The value can be used as the reference for name server software and operators to make decisions.
- Introduce a new resource record to carry the value.
Key points

● The meaning of the value.

● How the value affects DNS service quality level.

● Where is the value comes from.

● Procedures to initiate and update the value.
The meaning of the value

- The range of the value should be limited.
- A standard defines the meaning of each value.
- A practice recommendation on using the value.
How the value affects DNS service quality

Base on the value:

- Name server software can do some optimization like cache replacement policy.
- Operators can configure the black and white list.
- Monitoring system allocate resource.
- Name server software make decisions on reserving resource or abandoning queries when attacked.

...
Where the value come from

● DNS monitor and analysis system.
● Some companies (like Google) already have similar database.
● End user can give valuable feedback.
● Traffic statistics of DNS System itself
Procedure to initiate and update the value

- The value should be maintained by the domain registry side.

- In a totally open manner:
  - The domain owner will be notified;
  - The reason for the value modification will be recorded and can be fetched by anyone.
Miscellaneous points

- To provide rank value for the domain is optional not mandatory, so there is no backward-incompatibility and no breaking to current system.

- The whole idea is to provide an information sharing system, it is totally operational policy decision for servers to use it or not.
Miscellaneous points-cont’d

- If domain owners really don’t care about domain security and the portion of security-insensitive domains in one zone is quite high,
- Is it meaningful to do partial zone signing as an intermediate way to deploy DNSSEC?
Summary

- *Better* domain, *better* service, although higher price.

- Hopefully, this idea could trigger further discussions, we expect deep cooperation from different parties.

- Now we are focusing on DNSSEC, but there are still other problems in DNS world waiting for us to solve.

- From another point of view, we can see another world.
Thanks！谢谢
Q & A 请提问