RSSAC RSN WP Meeting @ IETF 95 15:15 – 17:00 Local Time
Participants: Brian Dickson, John Bond, Suresh Krishnaswamy, Paul Hoffman, Daniel Migault, Shinta Sato, Steve Sheng

DECISION:

- Work Party will resume teleconference every two weeks. The next full work party meeting will be on 18 April, Time to be determined. The work party meeting will focus on finalizing the list of naming schemes, and agreeing on its its pros and cons.

- The goal is to finish a work party draft for RSSAC caucus review in 6 weeks (by 13 May 2016).

- Suresh, Brian and Daniel to work on risk analysis.

- Paul to work on section 5 naming scheme.

ACTIONS:

- Paul to revise section 5 by 15 April, incorporating the working group feedback. Specifically, on the zone cuts and administrative issues.

NOTES:

- Roll call

Steve Sheng: Welcome to the RSN WP Meeting @ IETF 95

Steve Sheng: Google docs for the document
https://docs.google.com/document/d/1o6bPnz2_AF_LVv8_zRU9aQds95LKpq29F3XBGOSBx-I/edit?usp=sharing

Steve: Participants are Brian Dickson, John Bond, Suresh Krishnaswamy, Paul Hoffman, Daniel Migault, Shinta Sato, Steve Sheng. Apologies: Suzanne

- work party update (Steve)

Steve: Since we met last time, the work party has been in hiatus for a while. Since March, we tried to restart the work. Paul Hoffman and Suresh has joined the work party. Daniel M, Steve, Paul and Suresh has been trying to write some text to make progress on the document.

brian dickson: FYI I can hear fine
brian dickson: Yes, I will if I want to say something.

- overview of the changes in the latest version of the document (Steve)

Steve Sheng: Here is an overview the changes from this version of the document. At a high level, these are: 1) added introduction, 2) revised the terminology section to make it more readable, 3) added a brief functional description of root servers, 4) added brief history of names assigned to individual root servers, 5) rewrote section 5 analysis on naming schemes to make it clearer to the audience, 6) moved the analysis done on resolution complexity and response size considerations into Appendix, extensive clean up of those sections to make it more readable and suitable for publication. NOTE: we are not there yet, and 7) created a new appendix listing just al the dig outputs in order not to confuse readers.

Steve Sheng: What is missing. Sections 1-4 is almost ready. Section 5 needs work to lock down the naming scheme descriptions, its pros and cons, in particular how this naming scheme compares with appendix B schemes. The document also needs a solid risk analysis as well as findings and recommendations.

- discussion on the naming schemes (Paul Hoffman, Daniel Migault)

Paul has done a revision of the naming schemes, focusing less on zone cut and more on administration. The schemes are organized by starting with the current scheme and gradually removing dots in the domain name from the current schemes. The WP provided feedback.

John: It is important to retain the zone cut discussion.
Paul: I had some discussion with Daniel earlier today, and he mentioned that the discussion on administration earlier on the work party was discouraged.

Shinta: Having one dots vs. two dots. If having a zone cut if is in the root zone, root zone is managed by IANA, so in the root zone vs out of the root zone is an important consideration.

Paul: ok, then do you feeling having one vs. two zones cuts is important?

Shinta: If it is in the dedicated zone, it would be good.
Paul: Other thoughts?

Brian: The zone cut vs. no-zone cut is an important consideration.

Paul: Let's say signing is not important for the moment. Are there other advantages for zone cuts to focus on?

Brian: whether data is authoritative or not.

john: yes, agreed.

Brian: When the referral data is passed to the resolvers, it wouldn't be the case the resolver looks for the authoritative data. They would use it if someone asks, but they would not query for authoritative data.

Paul: that makes sense. So emphasizing zone cut is more about authoritative than signing.

Paul: I should do another round, and change the emphasis from who is responsible to there is a zone cut here or not. I can do a revision by next week.

ACTION: Paul to provide a revision on section 5 by 15 April 2016.

Paul: the other thing is about the shared single label. I have a scheme that was not considered in the original schemes. I know it was discussed and rejected, but could someone walk me through the discussion on this?

Brian: I participated in that thread. It was rejected for at least in BIND, if not other, the identity of the name server is tied to its name, not its address. If that addressed failed, then we have a big issue.

Paul: Is that an implementation issue?

Brian: it is implemented that way, but it is a huge number and long tail.

Paul: But we could describe the implementation status?

Brian: yes.

Paul: Ok, it seems that we should retain that option for completeness, and just tell why it is a bad idea.

Brian: To back to authoritative vs. signing.

Brian: Signing has value only if authoritative data is sought. If the resolver doesn't ask for authoritative, they won't get the DNSSEC signature. So there is no protection against spoofers.

Paul: But if this is a validating resolvers, the spoofer would send this to a zone identical to the root zone, or failure.

Brian: The basic problem is anybody can present data which matches the signed chain of delegations. If at any point, it goes to unsigned, then the end server giving those answers out send it own data.

Brian: If something is injected.

Paul: So this is not the the question for the data in the root, but making it easier for an attacker to attacker down the tree.

Paul: This should really be part of the risk analysis.

Suresh: if the single root server is serving both the root zone, and the first zone cut. then the nameserver is authoritative for both.

Suresh: when you query that name, you will get signature for both A and AAAAs.

Brian: That was correct, but it would be no longer correct because of the qname minimization.

Paul: That is not an issue with priming, right?

Paul: One of the things we don't discuss much is the scenarios under which we think these 7 proposal are going to be used.

Paul: Some of the assumptions we are making is that these will be used for priming queries.

Paul: If they sending query from cache, and if there is qname minmization, then we have an issue.

Paul: I proposed in section we don't deal with signing.

Paul: Under section 5 we will say who will do the signing A/AAAA.

Paul: Should I write something about the ownership of root-servers.net?

John: I think we should address that in this work party.

Brian: And I think there is value in that discussion.

Brian: In 5.2, NET is not signed by root.

Risk Analysis (All)

Steve: Let's move on Risk Analysis
Paul: what is the risk of signing root-servers.net?

John: Any known attack to the root zone needs to be addressed.

Suresh went through the risk analysis diagram and asked for feedback.

John: One thing i would like to do is to look at the impact of qname minimization in the lab tests we did.

Brian: This is a useful way to approach it. However, the binding between the risk and the naming scheme is not so obvious. we could do a summary table, across the top will be different schemes, each row will list one risk and have each schemes checked or not checked.

Brian: We can then do the risk analysis for the different schemes.

Daniel: Maybe we should split then, addressing signing vs. not-signing as one concept.

Next steps (All)

John: I think we need as a work party agree on the recommendations, and then on the pros and cons.

John: Then I feel we can go to the Caucus.

Paul: Would a month enough for us to go to Caucus?

People discussed, and felt six weeks is more reasonable.

The next teleconference will focus on finalizing the naming scheme options, the pros and cons. After that the next conference will focus on risk analysis as well as recommendations.

The experiment will also need to be rerun based on the naming scheme chosen and also factor in the qname minimization.