ABU DHABI – RSSAC Caucus Meeting
Tuesday, October 31, 2017 – 15:15 to 16:45 GST
ICANN60 | Abu Dhabi, United Arab Emirates

TRIPTI SINHA: —like what's the landscape going to look like five/ten/fifteen years from now. Clearly, that's one activity that we need to account for. From that, you typically draw an architecture of: Okay, based on this strategy, we would architect a service that looks like this.

Then, of course, policies would ensue from that, so we bat around some thoughts and put together a function which we call the [SAPF (Strategic Architecture and Policy Function) 00:00:27]. These are just components of what stitches together our mind map.

With any service – typically monitored and held accountable, so the root operators are looking at an accountability model for the future. One thing you typically do is have a cadence of constant performance monitoring. That's one event that we looked that all the operators should be involved in. At some larger interval, let's say, three to four years from now [Inaudible 00:01:05] three to four years into your operation, if you put SLEs and SLAs in place, someone needs to ensure that you're doing what you said you were going to do. Just like the RSSAC is being reviewed right

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

now, operators will be held accountable according to a set of operating procedures, and standards, and agreements, so we looked at that as well. When that would happen and how it will be fed into a larger accountability framework.

Then, there's the designation removal function. Thus far, there have been twelve operators that have operated this service, but, clearly, there will be some change in the future because this is not sustainable and also some may choose not to do it. So, we don't have a process in place to install new operators or decommission an operator, so we put significant thought into that as well and that is also being modeled in the mind map.

The last thing we discussed was financial function. Thus far, the operators self-finance the service and that, again, is also not sustainable, so we looked at what does it cost, what does it look like. Right now, most of our organizations treat the service as a [cost 00:02:21] center, and in this future model, what should funding look like? So we spent some time on that as well.

It's a very intense workshop. We've done some good work and the report is published. Go to the website and it's called RSSAC029. That, actually, concludes my very quick summaries of two reports. Any questions?

Yes?

ANUPAM AGRAWAL: Anupam from ISOC Kolkata. On the sustainability side, what was the view of the group? What were the key discussions which happened?

TRIPTI SINHA: Could you speak a little bit louder please?

ANUPAM AGRAWAL: On the sustainability issue, when you discussed, what was the key outcome of that?

TRIPTI SINHA: The sustainability of the service? Of the financing?

ANUPAM AGRAWAL: Yes.

TRIPTI SINHA: We don't currently have a sustainability model built into it. In other words, should someone want to decommission, we don't know how to decommission them, and how to on-board a new one. What is the view of the group? The group is in agreement that we need to look at how do we sustain this into the future? Now, this needs to move in harmony with the evolution of the

service itself and the technology, so we're keeping all that in mind. But, to answer your question, the view is it needs to be defined and we're putting some very sincere effort into defining it. I don't know if that answers your question.

Are you coming from a scalability perspective?

ANUPAM AGRAWAL: No, it is exactly the same because if you are facing this issue as a root server operator, it's the same issue which is there when we operate an instance as well. How do you sustain it over a period of time? I was looking for some linkages there that if you find an answer, I think—the root instance operators like ISOC Kolkata, how do you sustain it for the next three years? Because, currently, the bandwidth and all are supported by some ISP or the other.

TRIPTI SINHA: Okay, I see. I should have said something. We're actually at the 50,000-foot level right now, so you're going down to a more granular level, which is, okay, you've got an instance in a particular city, and it's fed by all these different ISPs, and it's resourced with this operating system, and so many use of servers and so forth, we haven't gotten to that level yet. We're at a very high cloud level and looking strategically into the future.

This will be produced as advice to the board. What you're saying is going to come down to 35,000-foot level, 20,000-foot level, that work is yet to come. But, that's a good question. Thank you.

Any other questions?

Alright, I'm hearing none. I'll close out this topic and I'm going to turn this over now to Duane who will give us an update on RSSAC028, and that's the technical analysis of the naming scheme used.

DUANE WESSELS: Okay. Thanks, Tripti. This is a document that has been recently completed by the caucus and we just wanted to go over it with everyone. The scope of work was to consider changes to the root server naming scheme and whether or not it made sense, what were the pros and cons of signing those names.

The work party considered these six naming schemes: The first one was sort of leave things as is, the second was to leave things as is except sign the [root-servers.net 00:06:40] zone. The third was to rename all the root servers into names that exist in the root zone itself, and by doing so they would automatically be signed. The fourth idea was a new top-level domain shared by all the operators. The fifth is like that except it's names that are delegated, so this is like a number of delegations to each

operator. The last one considered was to have a single label or a single name shared by all operators under which they would be the same number of thirteen v4 and thirteen v6 addresses.

The document spends quite a bit of time talking about packet sizes, response sizes, which is this table on the next slide. This table here is really a summary of what's in the report, the report has much more detail. The gist of it here was that almost all these schemes, we end up with the situation where the priming response gets a lot bigger, larger than fragmentation limits, so that implies that we're dealing with fragmented packets or an increase in TCP or so on. This work was done, not by me, this was done by Paul Hoffman and John Bond largely, and they tested these for implementations listed there at the bottom.

Partially because of the concerns around packet size, the primary recommendation from this report is no change at this time, that there are issues that need further study. One of those is to better understand how the current implementations behave with respect to signed data. The report references this node re-delegation attack, so a future work item is to better understand to what extent that attack is real or maybe different than other known attacks. The last recommendation was to explore options for minimizing the size of a signed priming response.

That's the last slide on this document, but I fully expect that there will be a call for new work to follow up on all these recommendations within RSSAC hopefully in the coming months.

Happy to take any questions if there are questions about RSSAC028.

ROBERT MARTIN-LEGENE: This is Robert. I was part of making this document. I'm kind of curious as to what now? As we see here, the outcome was to further studies, but who, and how, and when, and is this something we have some person doing a [doctorate 00:10:17] starting to do things or what's the idea?

DUANE WESSELS: No, I don't think so. My sense of it is that there would be another work party with a different focus on these particular recommendations or maybe different work parties for each recommendation, but I still see the work being done within RSSAC. I do think that, given the issues around the response size—one of the things this summary table doesn't really convey is that in some of these schemes, some of the implementations actually behave reasonably. I think that one way forward, dealing with the response size issue is maybe modifying or

making a new feature to the implementations to say, you know, give us the signed data, but don't do it in a way that blows up the response size. If we had that today, for example, that would have made the priming size not be an issue.

ROBERT MARTIN-LEGENE: Right. No, I know the issues. The best solution, in my mind, is the one that, sadly, has the biggest payload, but…

DUANE WESSELS: I'm sorry, say that again?

ROBERT MARTIN-LEGENE: No, I prefer the shared TLD solution, but it's the biggest payload, right? We cannot really start signing any of these without changing something, I think.

DUANE WESSELS: Right. Can you say why you prefer the shared TLD solution? Do you remember?

ROBERT MARTIN-LEGENE: Well, it would keep the existing structure with the name per root name server, which is, I think, is reasonable because a single shared name doesn't work and it would just move the

dependency of .net away from the root servers. Sadly, that brings all the signatures into the priming response.

DUANE WESSELS: Yeah, but, again, that can be solved with modifications to the authoritative software, I think.

LARS-JOHAN LIMAN: Lars Liman from NetNod. You can have the same names in the root zone without delegating. That's the first thing.

DUANE WESSELS: So, Robert's got a gut feeling that delegation is better. Okay.

BRAD VERD: If I may. We're going to have a call for work here shortly. I think these recommendations will need to become a statement of work, and a work party created, and start working on that, put it in the queue and start working towards finding answers.

TRIPTI SINHA: Alright. Thank you, Duane. Let's move on to the next topic.

Now discussion on work parties and work products. This is current work, so any cost instances. Kaveh? Is Kaveh here? No. Can somebody here who--?

BRAD VERD: I'll just add a little bit of color here – I touched on it earlier. This work party has essentially come to a close, it hasn't been finalized yet. The work has been gathered, it's been documented. There is a lot of documentation that the group has pulled together and that is being finalized. I was trying to get an update from Kaveh before I had to speak at the mic, but this work party has wound down and they'll be sharing their information here shortly.

TRIPTI SINHA: Thank you, Brad. Any questions about that?

Alright. [Liman 00:14:48] says no because he's very anxious to get on to his topic. Quick update from [Limon 00:14:52] harmonization of anonymization.

LIMAN: Thank you. There is an ongoing work party on anonymization of the queries. On a regular basis, the root server operators collect incoming DNS queries and upload them to our repository at DNS-OARC – you're probably aware of that, most of you.

Now, for those services who are based in Europe, we already have legislation in place that makes it difficult for us to combine

the information of the source IP address of the incoming query and the actual domain name that's being queried for because that is seen as integrity-sensitive data. A few of us have been anonymizing the IP address to make it more difficult to trace back and make connections back to the original query.

Now, we don't do that in a consistent function between ourselves, so we have now a work party that has actually three different tasks. The first one is should anonymization, meaning trying to obfuscate the IP address, would that be recommended? If so, how should it be done, which algorithm should be done so that we all use the same algorithm? That's kind of important if you want to compare data sets from one root server operator with another one. It's useful to have the same algorithm behind it, so you can see if the same query appears indifferent datasets. The third thing is should it be requested that all root server operators perform this anonymization regardless whether they are under legal obligation to do so or not?

So far, there has been a first cut of a document and it's written by Paul Hoffman who is the work party chair for this. We've received one set of comments from John Heidemann at USC, and there have been questions on – don't know if it was the mailing list or private mail. There is a first draft, but the meetings and the communication in the work parties are typically not

held as formal meetings. The person who asked if there are any minutes from this meeting, there are not because these are work meetings where there are discussions just to forward the content of the text, but there is a mailing list for this work party. I honestly don't know if it's archived or not, but I'd be happy to find out if someone wants to look at it. That's my update. Thank you.

Any questions?

Going. Going. Gone. Sold to the man yellow hat.

TRIPTI SINHA: Thank you, Liman. Alright, back to Duane. Duane's going to give us an update on packet sizes.

DUANE WESSELS: Yes. Another work party that's currently underway is an investigation of—again, I keep talking about packet sizes all the time. This is more issues around packet sizes from root servers. This one is focused on things like the points at which fragmentation should happen, MTUs, TCP, MSS, and whatnot. This was initiated, maybe, three or four months before the KSK rollover, sort of in anticipation of the time when we would have four key records published in the root zone and the size of that response would reach a new maximum.

Since that time, that has happened and, you know, it didn't melt. In that sense, this work party—there's a little bit less urgent need for this work, but it can continue. I should say, I'm the work party shepherd, I'm not the work party leader, George Michaelson is the work party leader, so he would be a good person to know and to contact if you want to get involved in this. There are currently discussions about having a work party in Singapore for anyone who will be at the ITF meeting, we may have a face to face meeting there.

Oh, yeah. Questions from anyone?

Okay.

TRIPTI SINHA: Alright. Thank you. Wes is now going to give us an update on some tools that are being developed to do analytics on RSSAC002 data the operators are producing.

WES HARDAKER: Alright. Really briefly. The RSSAC caucus now has a GitHub repository, http://github.com/rssac-caucus, and in it are a collection of tools. We're trying to find, sort of, a common place to put tools that are either being developed by the caucus or being developed elsewhere that people might want to use. In

particular, currently, we're very much targeting the RSSAC002 data, but honestly anything that the caucus needs to do.

In particular, there are three existing tools there now. One is RSSAC002 data, which is a place that you can just do a git-pool to get all of the history of all of the 002 data without having to go grab it from each letter by yourself. That makes it a whole lot easier if you want to do a lot of bulk analysis. There's an R API for actually querying through all the data and messing with it. Finally, actually, RSSAC028 – I can never remember numbers in my head – which is the naming study that we just talked about a minute ago. There is a bunch of test suits that were developed for that while that document is being written, so those tests were actually written in a GitHub repository as well.

You'll notice a few things. One, we have three tools so far. We could probably use more, so we'll come to that in a minute. For example, we have an R API, but we don't have a Python one, or an [Elisp 00:21:56] one, or I don't know what we need, but if anybody else that has code that might be used to either provide an API, or do analytics, or whatever, it would certainly be wonderful to add that to our collection.

My final question is back to any of you. What are the tools that you think might be beneficial or do you have anything you're willing to offer up to anybody else? What sort of analysis do we

think we might be interested to develop? We can create some smaller work parties or somebody can go off and do it. Does anybody have ideas of things they'd like to see or pieces that are missing?

That's okay. "No" is a perfectly good answer, but important part is to start thinking about it. That's it. Thank you.

TRIPTI SINHA: Thank you, Wes. I believe it's over to Brad now on a call for work.

BRAD VERD: Yes. First of all, I'll start with the RSSAC028 with the recommendations. Obviously, those are going to be taken. There will be a call out to the caucus to see if somebody wants to grab one of those things, create a statement of work, and begin work on that. If not, we will find somebody for those recommendations. If there's not a volunteer, someone will be voluntold, and we'll begin working on that.

We have had a talk with SSAC regarding that document and those recommendations. Both SSAC and RSSAC believe we want to find answers, so we need to bring those to a close. I just want to give people a head's up that that's going to be forthcoming. If you want to volunteer to create a statement of work, please let us know.

Then, obviously, a call for work, are there things that we should be looking into or should be brought up with the caucus? This is the place to do it. Please, are there suggestions? I see somebody running to the mic, so… Terry?

TERRY MANDERSON: Running's a pretty strong word. Say ambling quietly. There's a part of the root server system that isn't directly related to the root servers themselves, but is impactful. That's the name server selection algorithm in the resolvers themselves. Something I'd like to know and I would love for the caucus to work on is to do an analysis of what the algorithms in recursive servers are, how they behave right now, and is there a recommendation coming out from that – how they should behave in terms of name server selection.

BRAD VERD: Great. We will capture that, and put that together, and send that out to the caucus. Any other ideas?

If you're suggesting a topic, you will probably tapped on the shoulder to help with the statement of work, and then that will go to the caucus to see if the caucus believes that there is enough interest to spend time on it. Wes.

WES HARDAKER: I think this is the part where I have to profess my guilt because on my to-do list has been a topic to possibly write in a statement of work for so long. I have forgotten where it derives from and how old it is. At one point we wanted to look into what could a bad operator do – somebody with, I guess, evil intent. That's actually sort of a query for not, possibly, even just the root but for lots of stuff. The real question is does the caucus want to take on that work? Again, it's old. I don't remember where it came from, but should I consider actually writing up the statement of work? Does that seem like it still have interest to people at large?

BRAD VERD: Well, certainly. I think we should capture it and present it to the caucus as a whole. Not everyone is here to see if there is interest. I don't recall that one specifically, but it sounds like something we should send out.

WES HARDAKER: Alright. I will try and push it to the top of my to-do list instead of the far, far bottom.

DUANE WESSELS: Duane Wessels again. Is there something we should ask the caucus to do with respect to increasing the size of the root zone?

More gTLDs? We're being asked this question right now, I guess, but maybe that's a future work party item, do some explorations and studies around all that.

BRAD VERD: Great suggestion and certainly pertinent to what's going on with the addition of gTLDs and potentially more gTLDs being added. Great.

Anything further?

Alright. Well, we're not hearing anything further. The next thing is discuss previous work parties. I'm not sure who here has been on a work party, but this is to get feedback on how things went or how things are going if you want to share it. We're always looking to improve, always looking to be more efficient and make things better, so this is the time to give feedback if there is any.

No feedback? Alright. If you have feedback and just don't want to come to the mic, please send it to Tripti or myself, and we will take it into account, and apply it to our processes as we review them on a regular basis.

Tripti?

TRIPTI SINHA: Alright. There were no other items for today's agenda. This is my last call for any other business. Is there something pressing you'd like to discuss? Yes, go ahead, Anupam.

ANUPAM AGRAWAL: This is just to bring to the attention of the community the questions I faced which I never had an answer. The first one was that the government in my country used to believe that RSSAC caucus members are the RSSAC. There was one document which clearly divided the rules and responsibilities between RSSAC caucus members and RSSAC, so that was really helpful. That document saved a life.

TRIPTI SINHA: Saved your life? I didn't realize your life was under threat.

ANUPAM AGRAWAL: It was.

TRIPTI SINHA: Come on. You're going on record saying that.

ANUPAM AGRAWAL: No, no. It was. The second question which I did not have an answer was—the second part of the question was that how does

the main operator, maybe Verisign or ICANN, whoever is operating one of the instances, if you are operating an instance down below, what kind of security does the main operator ask you to do? Is there some kind of controls that there has to be a specified data center? Is the perimeter security good? What kinds of controls are existing or are asked for you to be maintaining all along when you are maintaining the instance? This, I never had an answer.

BRAD VERD: I can give you feedback for Verisign. I'm sure Terry has—maybe I'll speak—each of the individual operators who offer instances to all over the world or be run by hosting providers have their own set of criteria, okay? Verisign's is published on our website. You can apply, there's a review process, and it's not just a—there are physical requirements, there are network requirements, there are fiduciary requirements, not that you have to pay any money, but just that you're a viable business. These instances aren't going to end up in somebody's basement type of thing, you know, at their house, these are going to well-served areas. Verisign has a page. It's very well-defined for us and I will defer to the others for their own criteria, but I think they all have their own as well.

TRIPTI SINHA: Before I turn over to Terry, Brad is exactly right. Right now, the twelve operators, we all do it in different ways, but we have strong procedures in place. I don't know if that answers your question. Are you looking for something more in depth? Terry, were you going to say the same thing or--?

TERRY MANDERSON: Same thing exactly.

ANUPAM AGRAWAL: I'm aware of that because I signed the document with Verisign. I'm aware of that because I signed the document with ICANN for [Inaudible 00:32:41] What they were looking for is some kind of consolidated document, a broad checklist kind of stuff, which is mandatory for every [Inaudible 00:32:54]

TRIPTI SINHA: Okay. One, is there a consolidated document today? No, but all the operators do adhere to best practices. Alright, now, we are coming up with a best – what's the number of the document? I forget what it is, but we're coming up with that criteria. That's part of our future work, the 50,000-foot level work, we are coming up with an expectations document.

ANUPAM AGRAWAL: Thank you.

BRAD VERD: Yeah, there's an expectations document for potential root server operator that's happening, but, again, regarding the instances that you're referring to, each of the operators operate their cloud service in a different way. As was brought out in the tutorial and as stated here in RSSAC and in all the of the root operator's groups that diversity is a key factor for the reliability, the security, and the stability of the root system. As I said, each of those criteria, might be different depending on what the operator is. Having a consolidated list of what the requirements are for that instance, I would imagine is a little different here and there depending on which operator you're working with and that's by design.

TERRY MANDERSON: Absolutely. Building more on from that, even within an operator, and I can only speak for ICANN's root server at this point in time, is that it's a case by case basis. In some situations, we can go into a city with a very exceptional data center and in other situations, we have something less than that on a small island out in the Pacific somewhere, so we have to do it in the right

frame of mind that what we're trying to do is improve the root server system within the region where we're deploying.

In some cases, I won't get a data center that has security guards posted, that has biometric test for entry, I won't get a full 24/7/365 guaranteed power supply. It all goes very, very close, but there is not one universal mandatory line. There used to be an RFC that specified what the requirements were for a root server. It was outdated the second it was published and it was also, to an extent, that in some cases no one could fulfill. Yeah, it's a continuum. There is not one fixed position even within a root server operator.

ANUPAM AGRAWAL: I completely agree with the current situation and I support that also because situations can't be the same everywhere, but this is what I face as a question for which I never had an answer, so I was trying to raise it.

TERRY MANDERSON: What would help here is a document that specify, basically, what Brad, and I, and Tripti have all essentially said that there is a continuum – different operators do different things and within operators, things are done differently depending on situation. And that would help? Okay, thank you.

DUANE WESSELS: Two quick follow-up comments. One, some of these security checklists might just come out, say, a body of work that was tested to see what a bad operator could do. I don't know. I was just mentioning that a second ago, right?

Two, the wonderful things about—this is with my pro-DNSSEC hat on, which is a large part of my life or has been for the past decade. DNSSEC actually means that if something was insecure and started serving you wrong data, it would be detectable. That's the wonderful thing about DNSSEC. I don't want to say we'd put out a less secure instance, but it's detectable. That still doesn't mean that if they advertise a route that stops serving DNS that would be—that region would kind of go offline for that instance and other ones would have to pick it up. But, DNSSEC actually really helps out with the security effort because regardless of who is actually hosting an instance, the data is provably secure no matter who delivers it.

ANUPAM AGRAWAL: If the question would have been from DNSSEC and all, I would have been able to answer it. The question was the perception is that root instance is a critical internet information infrastructure of a country, so it has to be locked inside a big room with 24/7/365, five guards waiting outside. How do I answer that?

DUANE WESSELS: I think one important thing to pass on to people asking that question is that all instances are very carefully managed. One of the things that hopefully all instances should have is a very strong monitoring network behind it so that even if the instant went off for some reason, maybe there was power loss, it really doesn't matter, or maybe the name server software actually died, the monitoring systems that are actually watching all of those should be able to detect it and more importantly should be able to turn it off. The nice thing about any [Inaudible 00:38:50] instances is that if you turn it off, all the rest of them pick up, so it's actually almost totally invisible.

I take my sites offline, have you ever noticed? No, you probably haven't. You might pass that back to say—I don't want to say that you'd ever want it to just have it turn on and off randomly. The goal is to have it on as much as possible, but if it went off, it actually shouldn't affect the service seen by the rest of the world.

WES HARDAKER: I was going to say, it sounds like you have a need for documentation and that's really something that the caucus could produce. You could propose a work party around this and the caucus could write a document, something like advice to

organizations that host root server instances and we could totally write down what we're saying here or better.

TERRY MANDERSON: Okay, this is opinion only, my opinion only. I'm pulling out something you said in regard to the criticality of the root servers. They're not. They're important as having the mailman deliver your mail. It can be any mailman, it can be any delivery company, but there are other options, right? I think, that's one of the things we have to change this mindset that this is hallowed infrastructure, that it's somehow blessed. It's not. It's simple stuff.

ANUPAM AGRAWAL: I know that.

TERRY MANDERSON: I'm probably preaching to the choir, alright, but you need that documentation for other people. I get it.

TRIPTI SINHA: Thank you. Anupam, I hope that helped. You got a lot of responses from many, many people. We're all willing to help your case. We understand what your situation is. You get it, but you answer to other people who would like something more

concrete, and they frankly would like to point to a document is what you're saying. I like what Wes suggested – suggest this as a work item and have the caucus do something.

I'm sorry. Duane.

DUANE WESSELS: Yeah. One final comment. Thank you for asking. Because this is the type of discussion I think we want to have in the caucus, so those types of questions are great. It actually shows what real world needs are out there so thank you very much for the question.

TRIPTI SINHA: Thank you. Any other questions? Alright. That would adjourn the meeting. Thank you very much and I guess the next one's in Singapore for those of you who are going there. Thank you.

[END OF TRANSCRIPTION]