ICANN83 | PF – SSAC: RSSAC Community Open Mic
Thursday, June 12, 2025 – 13:45 to 15:00 CEST

KATHY SCHNITT

Thank you. Hello and welcome to the SSAC and RSSAC Open Mic for the ICANN Community. My name is Kathy, and I am the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy.

During the session, questions or comments will only be read aloud if submitted within the Q&A pod, or if you would like to speak verbally, please just raise your hand in Zoom or go ahead and raise your hand in the room and we'll open a mic for you. And we also have a handheld mic for those that are in the audience. Please state your name for the record and speak at a reasonable pace. And with that, I'm happy to hand the floor over to Ram Mohan.

RAM MOHAN

Thank you, Kathy. Welcome. And we're really pleased to have our brethren, our colleagues here. Also, this used to be an SSAC Open Mic Session, but we're starting a new tradition, right? An SSAC-RSSAC Open Mic Session. I'm really excited about it, Jeff. I'm Ram Mohan. I'm the chair of the SSAC. And--

JEFF OSBORN Jeff Osborn, chair of the RSSAC.

RAM MOHAN Okay, great. So, the format here for this session. Jeff and I will have just a few opening things. For many of you, it'll be stuff that you already know, but we often find that the people who come to our sessions don't actually know a lot about the SSAC or the RSSAC. So, we have a little bit of intro on that front. And I want to just take a moment and particularly say welcome to everybody who is here from the NextGen program, everybody who is here, the Fellows, all of you who are here. It's great to have you here. We appreciate your interest and the time that you're spending to come and listen to what we're saying.

So, with that, let's go to the next slide. This is what we're going to do, an intro to our two committees, and then it's your show. So, let's go to the next slide. SSAC, who are we? What do we do? So, we are chartered, the SSAC is chartered from inside of ICANN, and it links directly to the core mission of ICANN to ensure the stable and secure operation of the Internet's unique identifier systems. I won't read everything on the screen, but we are chartered directly from that area. We got started in 2001, right after the September 11 attacks happened, and we've grown from there.

Next slide. And we've grown from there. And the way we do our work is by engaging with the technical community, infrastructure

operators, analyze threats and risks to naming and address allocation services, and we coordinate with entities who are responsible for these functions. And we typically inform the ICANN Board about our activities, and we advise the ICANN community and the Board. We write reports, and most of our reports have recommendations in them. Some of them are actionable. Some of them are merely observations, but that's what we do, and most of our efforts are geared around putting ourselves together to generate reports that are meaningful and that have some level of impact.

Next slide, please. For the SSAC, we have five keystone issues that we focus on. DNS abuse, new gTLDs, DNSSEC, alternative namespaces, and the security, stability, and resilience aspects of Internet governance. Those are the five keystone topics. This does not mean that we are uninterested in other topics, but these are five areas where we have an enduring point of view. We have a body of work that we have created on these areas, and we expect that any time any one of these five areas comes up for discussion or if there's an evolution in those areas, you will find the SSAC involved, engaged, and intending to really contribute in those areas.

Next slide, please. Again, there's just a lot of text on the screen. I'm not going to go through it, but what this really is trying to say is that we've done a lot of work on DNS security, on domain name system DNS management. We have some seminal works on registration

data, and we also have published reports on routing security, on IDNs, among other things.

In the middle of the left-hand side of the screen, you will see a document that says DNS blocking/security, SAC 50, 56, 65. We just published an update to that document, and I see at least one of the co-chairs of that work party here, Warren, and so we published an update to DNS blocking as well. We've been presenting that at this ICANN meeting. While our remit is relatively broad, our focus tends to be around those five areas and provide specific, as much as possible, specific actionable advice if we can manage that.

Next slide, please. Here, SSAC 126, 127 is what I was just talking about, DNS blocking revisited. There's a link that's been posted in the Zoom chat. And we've also published SSAC 128, which is directly related to the RSSAC and what the RSSAC is doing, and we're strongly supportive of the direction that you're moving in, so those are the two most recent publications.

On the right-hand side of the screen, you will see our active work. We have three active work parties, one on DNSSEC operational considerations, a second work party that is moving to a close fairly soon, expect to publish in Oman. We have both work party chairs of the Free and Open-Source Software used in DNS infrastructure, the FOSS Work Party. We have the co-chairs of that work party also here. And the last one is—I'm not going to read the whole names, they are boring—it's the RIDE Work Party, and we have the chair of that work party also here, so if you have questions or comments,

we'll have the people who are helping coordinate that work together.

Just briefly, on DNSSEC operational considerations. The fundamental charter there is we're observing over time, DNSSEC has been deployed TLDs at the root and at lower down in the zone, and we find that there have been many instances where there are problems, and those problems lead to quite significant, in some cases, significant consequences. So, we're writing a document that both looks at those problem states, what they are, but also starts to provide some level of analysis of what may be going on and where DNSSEC may be appropriate to use and how, what are the considerations you ought to look at when you decide to implement DNSSEC. So, that's just getting started. We don't have a timeline for when that will finish.

Free and Open-Source Software, there's quite a lot of work that has gone into it. One of the interesting things that that work party has done has been to conduct a fairly far-reaching survey looking at how various parties who are involved in the DNS infrastructure, where and how are they using open-source software. And if there are some of you here in the room who are in this space, in the DNS infrastructure space, and you have either not been contacted with our survey or you would like to be listed in our report in terms of the open-source software that we that you're using, we encourage you to approach the one of the two co-chairs and we'll find a way to integrate your information into our report.

The responsible immigration of the DNS ecosystem is, I guess, a shortcut way of looking at it for the moment in time that we are in. It has a larger charter, but right now it's looking at the next round of TLDs, and the Applicant Guidebook has just been announced. And as some of you may know, the SSAC has published work on name collisions, and in this one is right now looking a little bit at security and stability issues that have name collision impacts, especially with names that may be in the blockchain space and that may have an interaction with the DNS space. So, that is just getting off the ground, but we're very cognizant of the timelines and the deadlines. Rick, how many days before the public comment is due? 42, Danielle says. So, we're cognizant of it. We're going to work on that.

Next slide. This is who we are. Still drawn mostly from North America and Europe, but we're steadily expanding the geographic representation. Membership into the SSAC is by invitation. You apply to the SSAC. You submit your body of work, what you have done, and the SSAC has a membership committee that reviews all the applications and shortlists candidates whom they believe will be able to make a contribution to the SSAC and who will likely also gain from being a member of the SSAC.

They then usually conduct an interview with those candidates, and typically one of the things that is expected is that the candidate reviews at least one of the SSAC publications and arrives at an independent point of view about what we've said on those publications. So, that's a minimum criterion, if you will. We want

to see not just your resume. We want to see what your intellectual contribution might be. We're diverse and drawn from multiple parts of the world.

Next slide. This is the leadership team. The way we work is in collaboration with the ICANN policy staff, and they have as much of a role in how the SSAC runs as we do. And it's a terrific team. It's really a lot of fun working with this team and moving things forward. Next slide. Over to you, Jeff.

JEFF OSBORN

Thank you, Ram. Again, it's really a pleasure to be meeting with you. I was jealous when I heard you guys did an open mic. I said, "we should do that." And the idea of doing this together made a lot of sense. So, again, we really thank you for it.

Next slide. Unlike the broad remit of the SSAC, our RSSAC's remit is very narrow. Our remit is to advise the ICANN community and the Board on matters related to the operation, administration, security, and integrity of the Internet's root server system. That's it. So, we are a committee that produces advice to the community and the Board. We are represented in great part by operators, but RSSAC itself doesn't actually do any operational things.

Next slide. RSSAC's composed of primary representatives from each of the 12 root server operators and an alternative. And then we have incoming liaisons from other bodies. So, that's 12 plus 12 plus 4 is 28. The larger body, the RSSAC Caucus, is made up of

volunteer subject matter experts. And 128 is the number up there. It's plus or minus some number, I think. Those groups get together and write a series of documents.

Next slide. Who can tell I didn't write my deck? That's all about correct, though. So, primarily, the caucus is a larger group that does work and gets together on the phone every couple of weeks or in meetings. We tend to be the IETFs and ICANNs as well. And it provides a framework for getting our work done.

Next slide. A recent couple of publications we put out were a security instant reporting one and a series of guidelines for what happens when you change IP addresses. Changing the IP address of a root server operator is something you don't want to do frequently. And it turns out that was quite a process to document the correct way to do that. Other topics that come up for review include one we're just kicking off, service expectations of the root server operators. The latest version we're starting now is Version 3? Three. And measurements, similarly, is something that comes up fairly often. 47 is an implementation of the way we did a lot of our reporting.

Next. And bearded, the gentleman on the left, that's me. And Ken, our co-chair, should be with us remotely. I believe he's in Maryland right now. We serve a two-year term, and it's a max of two years each. Next slide.

RAM MOHAN

Thanks, Jeff. And, Jeff, for the RSSAC caucus, do you have is it a rolling admission or is it time bound?

JEFF OSBORN

Thank you for asking. I'm not just the chair of RSSAC. I'm the chair of the RSSAC Caucus Membership Committee, so I can speak to this. We solicit input from the community, and we will take input and application from just about anybody. There's a place for applying on the ICANN website. One important notice is that because this is an expert body, we very often get people who say, I just learned about DNS last week. I'd like to be part of the caucus. And that doesn't help. So up until about two years ago, we would simply send a note and say, here's some good sources to learn. Here's some places you can figure things out.

And about a year and a half ago, we implemented a level of membership that is simply being on the mailing list. So now, instead of saying, we're sorry you're interested, we will probably say, it doesn't look like you necessarily have the background to be a useful participant in writing these documents. But if you'd like to sit on the mailing list, let us know how that works and let us know when you can come along and reapply, and we'd have you in place. So, it's a rolling process in the sense that every month we have a meeting. Every month we usually have at least one person. We literally allowed in our latest one hours ago.

RAM MOHAN Got you. Great. Thank you. yes, please.

DAVID LAWRENCE Hi. David Lawrence. I work with Jeff on the RSSAC Membership Committee and wanted to just add that one of the things that we do rely on very much as you do with SSAC is the aid of the ICANN staff in tracking things. And Ozan is our representative from Staff coordinating a lot of the stuff behind the scenes. And so, one of the other things like you, the RSSAC caucus depends on its members actually participating and are expected to produce. And so, one of the things that Ozan is very effective in doing is actually looking at people's participation on an ongoing basis, and then perhaps inviting people maybe to switch to the mailing list if they haven't been able to participate.

RAM MOHAN That's great. On the SSAC side, I had mentioned memberships and how to apply, etc. For the 2025 calendar year, applications deadline is June 30th. So, that's because we have to process the applications and go through the queues. So, June 30th is the application deadline. If you would like to apply or if you'd like to figure out whether you think you might have a shot at applying or whatever, talk to us, ask us questions, and information is available right on the RSSAC website. So, with that, we are in open mic session. Who wants to start? Jim?

JAMES GALVIN

I just wanted to note, you can't see this because they're behind you, but many more people have come in behind you since your opening remark about inviting NextGeners, and would appreciate if you would mention that again.

RAM MOHAN

You got it. So, for those of you who weren't there at the start, both Jeff and I, we want to invite, welcome all the NextGeners and all the Fellows who are here. We think you're a really important part of our community, and we are happy that you're here, number one. And number two, we welcome anybody who is sitting in the back who wants to come and sit here. There are still a couple of seats left. So come here and join us at the microphones. Thank you.

So, with that, questions are open. You can raise your hand here in the room, or you can put your hand up in Zoom. We have a roving mic available. So, who's got the first question? Okay, please. Identify yourself and ask your question.

UNKNOWN SPEAKER

Good morning, all. Good afternoon. My question is regarding SSAC membership. There is a timeline. I know that the deadline is the 30th of June, but how duration is the selecting of applicants and etc. Thank you.

RAM MOHAN Thank you. Great question. So, we're working on streamlining that to provide greater predictability on that. In general, I can tell you what the process is. Kathy, do you want to speak to the process since you're there? And Barry, you're here too.

BARRY LEIBA This is Barry Leiba. I'm on the membership committee, so I can tell you what we've been doing. The membership committee reviews the current SSAC members who are rolling off, who are ending their terms this year. And we've been doing that so far, waiting for all of these applicants, applications to come in by the end of the month. So, after the deadline, we'll start reviewing the current applicants and do our shortlisting and start doing interviews at that point.

We hope to get interviews done and get people selected by August so that we can get that to the Board, to the ICANN Board. Formally, the ICANN Board makes the appointments. So, the SSAC recommends to the ICANN Board who we would like to have appointed and the ICANN Board does it. And then we will have a SSAC workshop in September that we hope the new members can come to.

RAM MOHAN Thanks, Barry. Who's got the next question? Okay.

SUNCICA ROSIC

Yeah. Hello. I'm Suncica. I'm NextGen and I have background in data science and economics from Central European University in Vienna. I have a technical question. So, this morning we talked about DNS filtering and DNS blocking and that has been very insightful session for me, especially because I was able to draw connection to the concept introduced by Cristian Hesselman. And the concept in essence consists of a control plane approach to TLD stability and the idea of the system which is based on Entrada and Hadoop Distributed File System is to help threat detection based on DNS traffic.

Okay, I know that here I'm tackling two different things so the control plane approach is more like for threat detection and then DNS blocking is more like for filtering malicious domains according to my perception, but I was just wondering if it is possible to maybe integrate those two approaches so maybe use the output from threat detection system as a policy input to the DNS blocking so we can use it as an additional resource. Thank you.

RAM MOHAN

Got it. I see Wes and then John.

WES HARDAKER

Thanks. That's a very good question and certainly many internet service providers do just what you're talking about. DNS data in general is very sensitive and so most institutions are not willing to redistribute the results of their internal threat detection. That

being said, there are companies that sell lists of known phishing and DNS related names that have been spotted. PhishTank is one of them, PhishTank with a P-H is actually one of the more common lists that registers lists of names that people have gathered.

I have personally done a lot of DNS analysis and intrusion detection related things that have resulted in producing academic references for doing those detections. One thing you might look at is that there is a lot of available DNS data that you can sift through to come up with new algorithms if you want to get into the actual science of doing it and then apply it to live data streams when you can. But in general, it's very hard to come across data streams that you can do that live. But if you go look at, talk to individual companies, especially major network providers, you'll find that they're doing exactly what you're saying.

But as the blocking, the wonderful blocking and filtering presentation that was given by colleagues here, pointed out today, there's harmful sides in doing that. When you make mistakes, you end up blocking legitimate use that you didn't mean to do. So, you have to be very careful. And when you're trying to combine those two things to do automatic live detection, you're no longer having a human review it, which means that you're going to guaranteedly make mistakes because there's no perfect answer. Does that hopefully help?

SUNCICA ROSIC Yeah, that's a very concrete answer. Thank you.

RAM MOHAN John?

JOHN LEVINE Yeah, I was going to say, you said most of what I was going to say.

RAM MOHAN And you are?

JOHN LEVINE Oh, I'm John Levine. I'm on the SSAC. I would emphasize that this is, in fact, quite common, but the problem is since the bad guys can see everything that we can see, that the people who do this tend to do it in what-- They don't publish their algorithms. I work with a shadowy outfit known as Spamhaus, H-A-U-S, that provides lists of blocking advice. And some of their stuff is done manually. But a lot of it is done just the way you would expect.

And it's a typical example of the sort of stuff they do. They look for clusters of malware. If they see a name server with a certain threshold of, basically, if they see that half of the domains hosted on a name server are bad, they'll put the rest of the domains on the list because they figure the risk of making a mistake there is low. If you actually want to do stuff with this, I think Wes and I can both suggest people who you might be able to talk to who might be willing to give you some access to data. But it is finding ways to use

	the data and publish stuff that doesn't give away the secrets they don't want to give away will be difficult.
SUNCICA ROSIC	Thank you. Appreciate it.
RAM MOHAN	Thanks, John. Liman?
LARS-JOHAN LIMAN	Thank you. Lars Liman from Netnode and RSSAC. There's also a project in Sweden called DNS-Tapir as the animal, which is aiming at building a system for collecting anonymized data and focusing very strongly on the integrity problems and to build an analysis system with feedback from there, where the feedback is intended to be not a blocking instruction, but advice that a DNS resolver can use in combination with other sources of data to make a decision on whether they want to block it or not. So, DNS-Tapir is what you want to Google for.
SUNCICA ROSIC	Thank you for your contribution. I already took a look at it. My colleague from NextGen recommended me to the source. Thank you.
RAM MOHAN	All right. Who's got the next question there in the room?

RAFFAELE SOMMESE I have another comment for her.

RAM MOHAN Please identify yourself.

RAFFAELE SOMMESE Raffaele Sommese from University of Twente. We operate a large-scale measurement called Open Intel. It's a measurement of almost nowadays 80% of the second-level domain namespace. So, we collect daily data about various records of the DNS related to this domain name from DNSSEC to A and Quad A and NS record. So, if you're interested, come and chat. We are happily sharing data.

RAM MOHAN Thank you. Next question. Look, we've done this many times before. You just have to wait and then somebody will have a question.

WARREN KUMARI Also, it's also Thursday in an ICANN week, and I think people are fried, but I'm sure somebody's going to come up with something. It'll come. Thursday on an ICANN week--

RAM MOHAN There you go. Peter.

PETER THOMASSEN Yes. Hi, this is Peter Thomassen, SSAC. I have a question for the RSSAC or maybe for the SSAC too. Yesterday with, I think, Rod, I discussed, it was actually this morning probably already, we discussed the SCION routing technology. And I'd like to interact about that further with people who know more about that. So, it would be interesting to hear who knows the technology. It's a deterministic routing thing. And yeah, so.

WARREN KUMARI Yeah, I think you and I have both looked at it some. I've investigated some of it and there's a bunch of presentations in the IETF, in the MAP working group, I think a bunch of it. I'm sure we can find a bunch of presentations. It's apparently being somewhat deployed in Switzerland and a few other places. I think there was actually an SSAC or an ICANN presentation as well, but I can't remember. No, Tech Day. I think it was in Tech Day, but I'll look.

WES HARDAKER Yeah. Wes Hardaker from USC ISI and RSSAC, an SSAC fanboy. SCION is a very interesting thing, and I've wanted to explore it a lot more, but for those that don't know quite what it is here, it is a routing technology that's designed to keep packets within a trusted realm. And you can all sort of think of it as like a VPN overlay, but it's not quite that too. It's a brand-new architecture

that looks highly interesting and it is being brought forward into the IETF for potential future standardization, but it's very new at this point, which is why none of us here can speak to it.

RAM MOHAN And Wes or Warren, since you have some familiarity, perhaps you can post a link or something like that on the Zoom. Matthias?

MATTHIAS HUDOBNIK Matthias Hudobnik, SSAC. I just checked in the internet, so it says it's mainly utilized for a secure Swiss financial network and also some Swiss IX.

PETER THOMASSEN Okay. So, we seem to be having time, so I'm just going on, right? With more context or should I shut up? Okay, I'll just go.

RAM MOHAN It's an open mic, so you've got the open mic.

PETER THOMASSEN Okay. So, I've worked with the Swiss people on this thing, like superficially, and they initially wanted to use it to connect the participants of the Swiss stock market with each other and with central system. And then they've extended it to, for example, also include home office connections. And I believe one Swiss ISP has integrated support for that into their network, it might be

Swisscom or something, so that the bank's employees, when they do home office, they can use Scion. And that's pretty cool.

And so, the way it works pretty much is that you create sets of autonomous systems that you label a trusted, an isolated domain, I think is what they call it. And then you assume that BGP does the routing within such an isolated domain. But if you transgress an isolated domain boundary, you can say which ones of these isolated domains are allowed to appear on your path, and the sender can determine that. So, that means there's some flexibility about which way it takes, but also it's deterministic and you know which countries that are, for example, if you know where the autonomous system is deployed. And so, that's quite interesting. And I don't know. The SSAC does stuff about routing sometimes. And I just wondered if it's interesting for us.

WARREN KUMARI Yeah, I will note that when this was originally proposed, there was a bunch of discussion on there will be country level trust domains, and you will decide where your traffic can go in and out of a country, and there'll be basically gateways between countries. And that potentially doesn't align with a lot of the philosophy and ethos of the internet, where you have a trust boundary and the person who can decide whether something joins or leaves a trust boundary is a CA, probably a country level CA. And so, that's one of the reasons why there was a lot of initial concern from many of the IETF and other internet people.

Their design has somewhat changed and evolved over time to be more, you can be in charge of your own trust decisions, but there is still based on this isolation domain with a assumption that somebody will be in charge of deciding who can join and leave the isolation domain. But it's worth looking at some of the IETF presentations. I put a link to the Wikipedia stuff on SCION. There's a couple of good books. It's definitely an interesting thing, but the fact that it's used for, for example, the Swiss financial thing is to create a closed, intentionally designed as a closed network for security purposes. There's some correlation or maybe analogy between this and technologies like LISP, where you build an overlay with certain entrance criteria.

RAM MOHAN Thanks, Warren. In the queue is Ray.

RAY BELLIS Ray Bellis, ISC. I'm responsible for the technical operations of F-Root. Since you put that question to RSSAC and therefore it's a root system question, Peter, can I actually turn that question around to you and say, from what you know of the root system, why do you believe this system actually has applicability or potential applicability to the root?

PETER THOMASSEN Well, I don't know if it has. That was part of the question.

RAY BELLIS Okay. Well, yeah, we think probably not yet, but we'll see.

RAM MOHAN All right. Jeff.

JEFF OSBORN Okay, I'm going to respond to a planted question, but I also want to open a little with one of the things that's really challenging about showing up at a place like ICANN is you find yourself surrounded by some of the smartest people in the world who understand some of the most difficult subjects in the world and argue about them passionately. And so, you can walk into a room full of people and all you want to know is which side's the chocolate and which side's the vanilla. And they're telling you about the 15th amino acid and how it deferred from a chicken.

So, I'd like to start with a couple of basics here because it's stuff that people might be intimidated to ask. And there's a lot that's unknown about the root server system to an awful lot of people. So, I'm going to throw out a couple of them. One of the questions we get asked all time is, how much money do you make to operate a root server? Literally, because I want to make that big cash too.

Well, I operate a nonprofit called ISC. I'm president of ISC, proud and honored to do it. And we write software that we give away. We also give away in the person of Ray and his fabulous team, the root

zone. We provide the root zone information to anybody who wants it anywhere around the world in 287 locations, 350+ locations right now, and we are paid the princely sum of nothing to do that. We come up with the money out of the money that we make from giving away software to do this.

Okay. So, our vast mounds of coin come from giving software away and begging people to please help us with it. This is pretty universal across the whole root server system. There are some slight variances in it, but Wes is looking at me longingly there, but Wes has begged for money for his system as well as most of us have. So, I just wanted to-- This is a question nobody would have asked in a room full of really smart questions.

But who's paying for all this? Well, there are 12 organizations that primarily are paying for it out of their pocket. So, I'm hoping somebody was surprised by that or else I just wasted three minutes doing it. If you have any further information you want on this, I can talk on this all day. Another question.

RAM MOHAN Wait, there are other roots or operators who want to chime in on how they're both funding it and making sure that the system that they're running are stable and resilient.

JEFF OSBORN To be very clear, the last time you did a resolution, there was no coin to put a dollar into. This is all free at the point of service and

there's nowhere on the back end that we're getting paid. Oh, I forgot to watch. I'm sorry. Liman.

LARS-JOHAN-LIMAN

Thank you. Lars Liman from Netnode, another root server operator. I don't want anyone to walk away with the notion that the system is not financially stable though. So, there are 12 organizations that operate roots of operators. Each and every one of them has a financial plan for keeping and sustaining this system working quite well. Netnode, which is a for-profit company, private company owned by a foundation which is not for profit. So, we don't have requirements to generate a lot of profit to our owner.

We have a totally different plan for financing iRoot in our case. And that is a more of a regular business plan where we also sell DNS service and we earn money from that. Some of which we use to pay for the root service. And I know that other people around the table here have vastly different business models. And this is one of the various good strengths of the root server system that these business models are different. We are not depending on a single source of money to operate the system.

And also, should it come to a really, really bad situation where one of the root server operators no longer can fulfill the role of operating its part of the root server system as a whole, that is not going to have a noticeable impact on the system as a whole. So, these are two things I would like people to take away from this is that the system is financially stable and should it really become

really bad, losing a root server operator is not a major thing. Thanks.

RAM MOHAN Thank you, Liman. Hans Petter?

HANS PETTER HOLEN Yeah, thank you. Hans Petter Holen, RIPE NCC, operator of K-root. So, I would add to what Liman just said. The root server system, each of the root server operators have their own funding model. The RIPE NCC has 20,000 members that tips in to cover the roughly $1 million it costs us to run that system. You can see this in our annual report. So, we do this and are accountable to our members who are then ISPs, businesses in Europe, Middle East and Central Asia.

Other root server operators may be government institutions, it may be universities and so on, and they all have their individual funding strategies for this. So, I think it's not all of us, Jeff, that gives away free software to fund this, although actually getting money out of giving away free software sounds like a brilliant idea. So maybe I should look into that. Thank you.

RAM MOHAN Wes, do you want to come in?

WES HARDAKER

I mean, I can. University is certainly a hard thing to get money from. We get money from the overhead that we do on various research and it does drive our budget. I am probably less well-funded than some of my peers, but we have a very different model for what we try and do. We try and push the envelope and do new things. We are the only root server that currently offers TLS support. We've got to be different and to be to drive the industry forward. I could ask SSAC about TLS and the root. Come back to me about that.

I will tell one quick story, which is I was reaching out to a management company that measures the internet and tells how good it is. And one of the things they measure is the root server system. So, I asked him, "Could I get a free license? Because I'm a root server and we operate the service for free for the entire internet. And do you have any donations?" And the salesperson on the other end of the line says, "Well, let's talk about how are we going to increase your profit. What is your annual sales so that we can figure out how to increase that?" And I said, "It's negative." Dead silence on the phone, right? And to the end, they actually came back and they don't have a donation program, which was sad. But they had no way to fix the problem of we have a negative budget and always have for 40 years, right?

RAM MOHAN

Any other comments on this? Warren.

WARREN KUMARI

So, it feels like we've reached the Kabuki theater or leading questions bit. So, Jeff, the internet in my country is slow and that's because I don't think I have a root server. All of my queries go to the root, don't they? So, if I had a root server, life would be better.

JEFF OSBORN

I forgot to plant that question in the audience, Warren. I would like to thank you for having it. This is such a common misconception that it drives you crazy if you're involved in the root server system at all. If you look at a computer 101, communications 101 chart, it is possible to come away with the idea that in the beginning was the world and a world of dead computers and they knew nothing and somebody turned one of them on and the first thing it needed to know was I need a root zone to get going. Therefore, no life on the internet can do anything until there is a root zone.

That's kind of true, but it's incredibly misleading. You basically need it once and then you do everything else you do. We calculated that there are about 100 trillion resolver operations a day in the DNS around the world and one out of about 10,000 of them require the root server system. So, for the people who say all day long I have latency issues with my computer, why is your root server killing me so much? Let's think about how many times a day something needs to be resolved. A few hundred on a busy day, dozens. That means you have a root server lookup that's responsible for the latency on your computer something like once a month.

Okay, you tell me which of those 10 millisecond delays is my fault and I'll send you a crisp 10 cent coin to your home address to apologize for it. So, I think the basic idea is the root server system is not required in every operation, you need it once. And just to be really clear, the root server system provides so little information, it's incredible. I've been asked by really smart people, how dare you provide private information about my daughter's email on your root server system? And I let them know the root server system is a list of the addresses of where to look up what .com knows and what .uk knows and what the rest-- It's not even a whole domain name. All we tell you how to do is look up the thing to the right of the dot. And they say, okay, but why did you transmit that dirty picture that my son saw? I gave an address for a thing that isn't even a website. It's all we do. Does that help?

RAM MOHAN Thanks, Jeff. Next question from the room. Maarten?

MAARTEN AERTSEN Well, I greatly enjoy the theater. I would also like to have a moment's pause to see if there's questions from the audience. Because if we keep filling the air time, I don't think any will be. Ah, so there.

MOVITZ SUNAR Thank you. I'm Movitz. I'm in the NextGen with Suncica. I was just wondering if there's any collaboration between the SSAC and the CA/Browser forum or the PKI people and so forth.

RAM MOHAN Want to take that, Warren?

WARREN KUMARI Yeah. So, actually just around the time of the new gTLDs, the previous round, which was, I guess, 2012, there was actually a fair bit of interaction. Because the SSAC discovered that it was possible to get a certificate from the CA Forum for domain names which were not yet delegated. So, for example, if a TLD like .page didn't exist, one could go along to the CAB forum and get a, at that time, 5- or 10-year certificate. These were called internal name service certificates.

And so, that obviously would interact poorly with the new gTLD round. And so, we had a bunch of discussions with the CAB Forum. There was actually, I think we published an advisory on it. This was SAC57. The CAB Forum agreed that this was suboptimal and made all of the CAs, which were their members, go through and revoke all of the existing certificates for these internal name sets. I don't think that we've had any other formal discussions or interactions with the CAB Forum, but we do have a number of people who participate in multiple places and chat. But I think, did we forget one?

RAM MOHAN Let me manage the queue. So, Peter?

PETER THOMASSEN Yeah. So, as Warren said, there is no formal interaction, but there is some practical overlap. It's like an adjacent community in a way, and some people are active. Or Russ Housley, for example, is in the SSAC, and he's also a web PKI expert, and he's not particularly part of the CAB Forum, but I would suppose he knows almost everyone there. And yeah, so that's how it works.

And so, sometimes topics come up. For example, the CA Browser Forum currently has a proposal to stop issuing certificates for domains under .ARPA because those are not supposed to be websites, is the main argument. But that might lead to unintended consequences. So, some of us have reached out and are trying to think this through more, but that's not an official SSAC activity. It just happens to be an overlap of people. Do you ask that question with a particular motivation, or is it just curiosity?

MOVITZ SUNAR So, it's mainly curiosity. It comes from I talk about subdomain takeovers. And I've been a lot in, for example, the CT logs for gathering domains and so forth, and scanning for these problems. So, I've been in both of the areas between DNS and certificates. So,

I just thought it was interesting to hear your thoughts and if there's any future problems that you see in this overlap.

RAM MOHAN Thank you. Ray, and then John.

DAVID LAWRENCE I'm David Lawrence. It's okay. I just wanted to say there was a reference to SAC 57, and so for the benefit of the NextGen and newcomers to this area, both the RSSAC and the SSAC publish its documents in a library, and so SAC 57 is referenced to a particular report that was written on this topic. There is a large library of reports produced by both groups that are publicly available, and it's like the RFC series from the IETF. If you're looking for more information, you can read through these reports and see all the considerations that have gone into it.

RAM MOHAN Thanks, David. John?

JOHN LEVINE The more I think of it, the better a question that is, since, as I'm sure you're aware, we all get our certificates from Let's Encrypt, and Let's Encrypt's validation is, in fact, a single unsigned DNS lookup. Now, they do it from multiple places to make sure that it's not being spoofed in obvious ways, but the security of CAs in reality these

days is the same as the security of the unsigned DNS, so that's definitely a topic that perhaps we should think more about.

RAM MOHAN Thanks, John. Maarten?

MAARTEN AERTSEN To the best of my knowledge, they use unbound and have DNSSEC validation on, so there's some nuance to what you just stated as absolute truth.

JOHN LEVINE Well, you are correct for the 6% of the domains that are signed.

MAARTEN AERTSEN Sure, sure.

RAM MOHAN Okay, next question. Please.

RAY BELLIS Ray Bellis, ISC. How much work has SSAC done on the routing aspects of the root system and DNS as a whole? Leading on from the reason I asked, leading on from Warren's earlier planted question, something I've experienced running R-root is that routing is really actually the crux of the matter in many places. I can give a good example of a particular country in Equatorial Africa where

there are two IXPs, and it happens that we're present at one of those IXPs, PCH is present at the other one. Most people in that particular country actually get their Internet off a mobile network operator.

So, there's a big national carrier, but that big national carrier doesn't actually understand the root system and actually won't peer with the root server operators there, and therefore they actually don't get the advantage of having a root server or indeed multiple root servers near them topologically close, and in terms of latency terms, not that latency matters that much to the root, as we just heard, but they're not there. And if you're not peering, you're not going to get those root servers. So quite interesting. What, if anything, has SSAC discussed that as its area for research?

RAM MOHAN

Sure. If you go to the SSAC page, you'll see there's an entire page of documents on both the root server system as well as addressing. But I have to say that in the last perhaps three or four years, we've spent more time commenting and providing advice on the naming part of the system than the addressing part of the system.

WARREN KUMARI

Actually, can I add to that? We published SAC 121, SSAC Briefing on Routing Security, which talks about RPKI and ROAs and similar. And then a more recent document was SAC 125, SSAC Report on Registrar Name Server Management, and that discusses if you run

a name server, you should keep your name server secure, but also talks a bunch about make sure that people can reach it, make sure you're monitoring your routing, make sure that people are actually setting it up and understand routing, etc. We have some documents. There could definitely be more.

RAY BELLIS Yeah, I've seen those. I'm thinking more of something from SSAC saying, please peer and peer widely. Look at where the root servers are, and please adjust your peering policies and peering locations accordingly.

WARREN KUMARI These documents were all about protecting your name servers. We've trusted that the root server operators have got the other part of it in hand. Like you all have demonstrated good ability to provide good any cost, good security, and we think probably people who want good connectivity to a root server likely will be talking to you.

RAY BELLIS One would hope, but that doesn't seem to happen.

RAM MOHAN So, Ray, maybe there's some work to be done together between the RSSAC and the SSAC.

RAY BELLIS Well, I have applied to join SSAC, so perhaps if I get in, there's something we can talk about.

RAM MOHAN Yeah, sounds good. Russ?

RUSS MUNDY Yeah, I just wanted to second what Warren said a little bit ago for the publications, but there have been what I'll describe as limited discussions about routing-related topics over the years of SSAC and really quite limited discussions about routing specifics related to the root server system. But it is an area that I think could deserve some increased attention, and there might be useful things to be said in either an SSAC or an RSSAC publication, and it's something that might well be worth working on jointly between the two groups. As the liaison between them, I'm happy to help.

RAM MOHAN Thanks, Russ. Other questions from the room? Please.

ROB GOLDING Yeah, Rob Golding. It was a question about the geographic breakdown of the current RSSAC. There was a significant lack of the Latin American participants. Is there genuinely an actual bias in terms of culture, language, and location over how they view

Internet security? In which case, should you be going and hunting for people in that region rather than waiting for them to apply? Or is security so diverse already that language, location, culture are not actual barriers, and so it's not a problem having so many that are North American-based?

RAM MOHAN

And that was a question for the SSAC? Yeah. Okay, that's a question for the SSAC. We don't have Tara here, but Barry, do you want to take that?

BARRY LEIBA

Well, the first thing is that we are actively looking, so that's true. At some level, technical security issues are technical security issues, but different views give us perspectives from different regions as, are there issues in your region that the rest of us are unaware of where we think we don't have to worry about X, but you know what you do have to worry about X because in Africa or in Latin America or whatever, we have these problems. In remote areas, we have these problems. All the rest of you are in cities.

So, there are variations on the technical issues and how applicable they are that we need the perspective on. So, that's why, and then there's just the general thing that an organization with multiple views works better. So, that's the thing, but we actually have done outreach, and we will continue to do so.

RAM MOHAN And if there are people listening in who are from any region of the world, and you can contribute, put your applications in.

BARRY LEIBA Right, help with the outreach is always--

RAM MOHAN Yeah, we need help with the outreach for sure. And please look at the email. You can just email us directly here as well. Who's got the next question? Please.

ADRIAN Hi there. It's Adrian [ph] from DNS Africa. So, this one, I'm not sure how critical it is, but it was just something I thought was interesting, so I thought I might mention it. My recent task was setting up a new RDAP server to comply with the newest February 2024 ICANN response profile. One thing that I've noticed comparatively to WHOIS is the growing size of the RDAP requests, especially when you start looking at the redacted. You have this massive RDAP request, but you're only looking at like two or three lines that are actually useful.

And one of my wonders was I was reading some previous SSAC publications, and one of the things was that be very careful with rate limiting. And my thing is that would may be reducing the size of an RDAP request allow you to query more RDAP in a sense? So,

you can say we take out a bit of the fluff, and that will allow us to hit the server a bit harder. So, it's kind of a tradeoff.

RAM MOHAN Who wants to respond? David?

DAVID LAWRENCE So, one of the interesting things about network denial of service attacks is often that the pure volume of requests and responses is not really the issue so much as the packet rate. And so, shrinking the size of an individual request or response doesn't have as much of an impact on the effect of a DOS as you would imagine, because it's really the line speed of the network that can use a physical network that really impacts the effect on both the servers and the network itself.

RAM MOHAN Other responses? Rod?

ROD RASMUSSEN Yeah, so there has been some of our SSAC members have done some studies.

RAM MOHAN This is Rod Rasmussen.

ROD RASMUSSEN

Oh, Rod Rasmussen, SSAC member, sorry. Have done research on related research, which has then focused them on looking at rate limiting. Rate limiting is not, by and large, is not a problem of network congestion or the like. It's because of policy of registrars restricting access. When you get one query per day, that pretty much is not a DDoS response. It's a policy response. Thanks.

JAMES GALVIN

James Galvan, SSAC. In a more operational context about rate limiting here with respect to RDAP, even on the ICANN side, one of the things that's interesting is ICANN policy doesn't really speak about whether or not you should or should not rate limit, and in any case what that should be. But individual registries and registrars do often step back, and their infrastructures they do what they do. They have to make their own choices about protecting their own infrastructure, and so they may create their own policies about rate limiting for the purposes of this is their RDAP infrastructure, and if they believe that they're getting a single source or an overburdened source towards them, they might want to do things to protect all of that.

SSAC has spoken about this rate limiting issue. It goes back a while, SAC 101, I think it was. And I'm getting some nods, so I guess I got the number right. We did speak about rate limiting issues, and it's a problem from a researcher point of view. It's a problem from a security practitioner point of view. Sometimes you get at data, but it's a one-to-one. It depends on who you're trying to reach and

their own demands for themselves, but there's no specific policy within the ICANN arena that makes you do things a certain way, but you're given the privilege of doing something. So, as Rod said we as SSAC do care about this issue because it does affect security practitioners in particular, so we just keep awareness about that. Thanks.

RAM MOHAN Who's got the next question? All right. Let's check if there are any other questions online. Last call for questions.

LEONARD HAUSE I have a question on, since you got a big crowd in here. I'm Leonard Hause from US. To what extent are there formal processes or consultations on changes, adds, changes, deletes within the regional Internet registries?

RAM MOHAN Who wants to take that? Could you please repeat the question?

LEONARD HAUSE Formal processes from either SSAC or RSSAC with changes with the regional Internet registries, like adds, changes, deletes.

HANS PETTER HOLEN So, I'm operating a regional Internet registry, and I'm not sure what you mean by a deletion in the regional. Do you mean removing of a regional Internet registry?

LEONARD HAUSE Or addition or change?

HANS PETTER HOLEN So, we've had in the history of regional Internet registries, we've had addition of two through the lifetime of ICANN. Before that, three were established, and that was done by a collaborative process with the community and the RIR. They split out from the most complicated one, came out of three RIRs, and they were set up.

Now, the world is more complicated today than in 2002, 2003, and 2005, when LACNIC and AFRINIC was set up. There is currently under discussion a process for not only accreditation, but also ongoing commitment and possible deaccreditation of RIRs. Now, I don't think-- That process is ongoing. The ASO Address Council has met and discussed at this meeting the comments that has come to the first draft, and there will be a second draft out later this year. And that will be discussed at the RIR meetings and at the ICANN meeting this autumn.

At that point, I think risk assessments and looking into how that would affect other services would be appropriate. But at current, to some extent, the RIR is just a catalog of who uses which IP

addresses. The Internet keeps running, even if we're not there. No, it's not quite that easy, but for the day-to-day operations, I think that's a good starting point.

LEONARD HAUSE: Yeah, I was just wondering if that had been documented within the SSAC or RSSAC at some point. Thank you.

WARREN KUMARI: And I guess a very short, quick addendum to that. The SSAC, and I think it was last week or the week before, published our latest advisory, which provides input to the ICP-2 process on recognizing and derecognizing RIRs, largely just supporting the work that the RIRs have been doing.

RAM MOHAN: Liman?

LARS-JOHAN LIMAN: Liman from RSSAC here. I was just going to say the same thing about RSSAC. RSSAC has also submitted a supporting comment to what the RIRs are doing. Thanks.

RAM MOHAN: Okay. Any other questions in the room? None online. I'll give it another 10 seconds. Okay. That brings the questions piece to an end. Jeff, any closing comments?

JEFF OSBORN Yeah. Ram and I were talking about this before. Sometimes it's hard to ask a question in a big setting like this with a booming microphone. So, if you take a look at us, most of us are really nice people who love to talk about this stuff. So, if you see one of us around and you wanted to ask a question in private, if we don't know it, we probably know the people who do. So, I'd highly recommend if you had a question, look for one of us. We love this. This is a volunteer thing for almost the most part. This is something we do, volunteer on our own time. I'd rather be sailing with my kids, but I flew around here and I do this. So, if you want to know something, find us and ask.

WES HARDAKER Good luck getting us to stop talking. That could be a different problem.

RAM MOHAN Thank you all. That concludes this session.

JEFF OSBORN Thanks, Ram.

[END OF TRANSCRIPTION]