ICANN75 | AGM – SSAC Public Meeting
Wednesday, September 21, 2022 – 9:00 to 10:00 KUL

KATHY SCHNITT: Thank you. Hello, and welcome to the SSAC Public Session. My name is Kathy, and I'm joined by my colleague Danielle, and we will be the remote participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in chat will be read aloud if put in the proper form as we will know in chat. If you would like to speak during this session, please raise your hand in Zoom. When called upon for virtual participants, please unmute in Zoom.

For those on-site, we will use a physical microphone to speak, and please remember to leave your Zoom microphone disconnected. For the benefit of other participants, please state your name for the record and speak at a reasonable pace. You may access all available features for this session in the Zoom toolbar. And with that, I'm happy to hand the floor over to SSAC chair Rod Rasmussen.

ROD RASMUSSEN: Thank you, Kathy, and welcome everybody to our open SSAC meeting this morning. Glad to see you all here. I guess, typically, this would be the morning after the gala, no gala, but I think there may have been some gala going on anyways last night. And it's always a tough one to have the first one in the morning after that, but I appreciate y'all being here and hope you bring some good questions to the SSAC.

Actually, can you have the next slide for the agenda, please, Kathy? We're going to run over our recent activities and give an update on the named NCAP, Name Collision Analysis Project, our ongoing work parties, and then talk a bit about new members. We're starting the period where we're taking in applicants for that.

And I'm going to start it off with an overview of the SSAC for those of you who may not be familiar. And I hope we get some ICANN fellows either in the room or remotely because this is an opportunity, especially for those I've met a few so far, this meeting are very in the security field. And I hope one day to have many more fellows represented up here leading this as old timers. I can get retired off to take on the next gen of this work.

So could I please have the next slide? So what is the SSAC? We are committee that reports to the ICANN Board, actually officially appointed by the ICANN Board, but we'd self-select our membership and they review that and approve those members. There are 36 people right now that represent a wide range of operational and security experience. Typically, we have amongst our membership many years of experience and responsibilities that we've had over the course of our careers, and we bring that knowledge, expertise, contacts, etc., to the ICANN community. It's a volunteer organization.

And as you can see on the, what is our expertise? We have a wide range of things we look at. We actually have an even longer list of that for attributes that we look to recruit. And I think Julie will talk a little bit about that when we get to the recruiting section. By the way, I'm Rod Rasmussen, the SSAC chair and Julie Hammer is our vice chair. And that's our pleasure to be able to be here today.

So what we typically do is look at various issues and things and provide reports publications. 121 and official SSAC documents since 2002, and you noticed that's 20 years ago, and we're coming up on our official 20 year anniversary very soon, which we'll be celebrating. And we've been talking a bit about that recently.

It was the original SSAC was formed as a President committee on security right after 9/11, and that quickly evolved into the SSAC. And our role is to advise the community and especially the Board on all manner of security and stability issues, and particularly around things that are threats to the integrity of the identifier system.

Next slide, please. So as part of ICANN's overall mission, and the fundamental part of their mission is to ensure, and is right in the front, the bylaws ensure that stable and secure operation of the Internet's unique identifier systems. And we are one of the primary parts of the community that that focuses on that area.

There's a lot of other parts down as ICANN has evolved over time. OCTO, the office of the CTO has got a lot of capabilities now. And when SSAC formed, there wasn't a lot of expertise out there in the industry that is this very prevalent now. But we'd have far more folks to draw from and more interesting. The issues keep evolving and they are always interesting to look at.

So the way our process works is that we have an issue and it could be something the Board asks us to look at, like, the NCAP project, we'll talk about in a little bit, or something that we develop internally or public comment or something like that. We form most what we call a work party. And that's a group of interested members.

And typically, they have a background and expertise in an area of security or stability, etc., that we can pull those together in combination with our staff and potentially outside experts that we occasionally will bring in to a work party. We will work on that issue, whatever it is. We'll do a lot of research and then we'll start writing up a report within that work party. The work party will review it internally and then present it to the entire SSAC for a full review of the SSAC.

Oftentimes, we're looking at a very focused specific issue where some of our members may not have the expertise, but they can take a look at it with an eye towards, does this make sense to the rest of the community, etc. So it's a really good process for bringing focus in from experts, but not experts in that particular area to review that.

We go through that processes and sometimes we iterate back and forth as issues that the full work SSAC may see or get dealt with by the work party. And eventually, hopefully, not always, but most of the time, we publish a report that then goes out to the community. And sometimes those reports include recommendations often to the ICANN Board and there's an official process for that where they take those in.

This is the consideration. The advice here we submit that. If there's advice to the Board, they take a look at it. There's a whole tracking process that goes on where they take a look at it, make sure they understand it. They go back and forth with us to making sure that we're all on the same page as far as what we're talking about, what we're asking for, what we might be recommending.

Some of these things may be get referred off to the policy process and the GNSO or ccNSO or elsewhere, or even external parties.

We've had recommendations that are as part of the identifier system that may not actually be part of in with an ICANN's realm, but IATF or others may have a role on that. So they may get referred off to there. The Board itself though has an obligation to respond and work with us to some sort of conclusion on the issue whether it's going to be implemented, or not, or if it might be modified, etc.

So there's a process that goes on and sometimes it's very quick, and sometimes it's years, and we have some things that are still not, they are still out there because things take time to develop and work on. And we track those over time as well. But the way, if the Board declines to act on our advice, they do notify us of that and the reasoning for that.

Next slide, please. So we have the most recent publication we we've put out, SSAC121. The hundred and twenty first document of the official series. And that is on Routing Security. And this is an example of a more of an informative document where we didn't have specific recommendations to the Board or any particular organization. However, as you'll see, and we're going to go through this, it has a lot of advice in within the kind of the framework of it to operators as the DNS and how they may be threatened by routing security incidents. So we'll go over that here shortly.

And one of the things we've put many reports out on, SAC120 being the latest is IDNs of various flavors. And we had an Addendum to SSAC114, which was looking at, and that's getting back a little bit of time now, that's beginning of the year, we're just looking at our comments on the subsequent procedures work. So those aren't recent publications. And there's some information there and will be available if you go to the website to download about how to find these things, but it's pretty straightforward to go to the website and or even just Google it for SSAC publications, and it'll pop up.

Next slide, please. Okay. With that, I'm going to hand this over to Russ Mundy, who is remote, to walk through SSAC121, our briefing on routing security. Russ.

RUSS MUNDY: Thank you very much, Rod. And thanks for that intro that it did well define that this particular document is not a document that contains recommendations for the Boards or explicit recommendations for other activities. But as you say, there aren't recommendations, there's really advice and suggestions to those involved in the DNS realm and in the routing operations realms.

So next slide, please. There's really five areas, five main areas in the document itself. And this presentation is very much a direct extract from the content of SSAC121. And so you can see that the five areas there. And let's go to the next slide, please. Thank you. So this is an illustration right out of the document. And it was something that was developed as part of the work party activity to try to bring a graphical illustration of how the DNS system and the routing system are interacting with each other all the time and on an ongoing basis.

And in this picture, what it's showing starts on the small device that maybe looks like possibly a cell phone on the left or something like a tablet or something. And that device generates a question or is recursive resolver, which you see is sort of in the center. It's resolver D. And it's asking, where is example.net? This is www.example.net. So this is a very common way to show how the DNS is functioning.

So what is the top error? It would show what happens from a DNS perspective. So client C, ask resolver D, and resolver D is a recursive resolver. So it goes and asks as many DNS authoritative resolvers as it needs to get an answer to the question. So the DNS server, authoritative DNS server, hey, gets the question, provides the answer, goes back resolve the D, and resolve the D answers client C.

However, that's not really the full picture of what happens. What actually occurs is packets are moving around the Internet and below that horizontal line in the middle is an example of how the packets are actually moving through the Internet between the DNS element that I just described. So when the client C places his request, it goes to AS1, through AS2, through AS3, to get to resolver D. So that's the actual packet flow.

So in other words, it doesn't go directly from the client C to the resolver D. It passes to the Internet and passes through routers and switches, and there is devices out there. And same thing for when the resolver D goes to authoritative server A. It passes the data through the Internet. And in that case, it goes AS3, AS6 over to DNS server A. And then the answer after these transactions occur comes back and the answer is one 192.0.2.1. And so that's the answer the client C gets for using to get to www.example.net.

Next slide, please. So this is an illustration of how a routing event, routing anomaly, you could call it a routing attack, occurs and interacts and ends up with the incorrect answer getting back to client C. So the operation begins the same way. Client C asks the question or send it to AS1, and instead of going to AS2, 3, and going right to the resolver D, it actually gets diverted to AS4. A4S sends it to a malicious DNS server, which responds with an invalid answer going back to client C. You'll notice the answer here, this slide is 203.0.113.1. So different than the last answer. And so that is a relatively simple example of how a routing attack can be used to give a false and incorrect answer to a DNS query.

Next slide, please. For the most widely recognized attack of this type that it was a routing attack that was involving targets that were, in this case, the target rather did involve some use of DNS as well as routing. And so the attackers injected information into the routing system that the end effect was that the packets that were asking DNS queries for MyEtherWallet went to an invalid or a malicious DNS responder. And the bottom line that is widely seen and written up in the descriptions of this attack is that the attackers stole $150,000 dollars in Ethereum in about two hours-time.

But perhaps just as important is that for those two hours-time, all of the other customers of the Route53 DNS service were effectively out of service. They were not getting any DNS responses. And so this had a very much twofold negative impact. One was the stealing of the Ethereum, the funds in Ethereum. And the second was that the DNS service for Route53 users did not work for those two hours.

So next slide, please. And so what are the things that make it feasible to execute this this type of event. So in most cases, the authoritative DNS servers will answer any queries that they get. Somebody asks that's what their purposes are authoritative and they get a question for it, they answer it. Many and a large proportion, very large proportion of DNS clients do not authenticate the server that provided the answer, nor do they in the end client do DNS validation. Therefore, they, at the end client perspective, have no reason to have or have no strong authentication of the information they received and they just act on that information regardless.

And additionally, almost a very large proportion of DNS queries are still very much unencrypted in the open UDP packets so they can be intercepted, they can be replaced, and responses can be tailored to accomplish what the bad guys want to accomplish. So the routing attack then can substitute one DNS server for another. Routing attacks can alter the path of the query, and they can observe the DNS queries. They can collect information on DNS and other applications. So there's a number of facets that make this a viable situation that can occur with some regularity.

Next slide, please. So this slide is really a summary of the enhancements that are described in the routing security briefing from the SSAC. And I won't go into it in a detail here because we have more slide on H1. So next slide, please. So the routing registries were something that was put into practice a fair number of years ago. And what they are intended to do is to provide a place to not only collect information, but provide information to those using the routing systems so they can get the large amount of data that describes how routing is to be done spread around and provide in an efficient way.

Now, the routing registries are not in general coordinated entities. There are a lot of different routing registry. Some of them are operated very effectively and are watched very closely, manage very closely. Others are not. And it's also a pretty common situation for information in one routing registry to be different than information in another routing registry.

Next slide, please. So the resource public key infrastructure, RPKI, is in some ways, an effort to provide a much stronger mechanism to provide a means for cryptographic verification of information similar to what is contained in the routing registries. It is structured so that it follows these allocation of the information that's used in the routing system and those that are doing RPKI participation and validation. Not only can put things in and then have that information used and validate it cryptographically by those that are getting the data out. You get a much more consistent picture than you do. The routing registries allowed.

Next slide, please. So this is a description of the set of things that from an operational perspective are really necessary for anyone that's involved in routing, running a fairly sizable routing operation. And in many DNS specific places, do also operate a fair bit of routing as part of the DNS service.

And the monitoring that's described here is both internal monitoring, both inside of your network to make sure that the packet are going where they are supposed to be going, or where you think they're supposed to be going. And then external monitoring is how the rest of the Internet from outside of your network is treating your packets. And you need to have reasonable idea that they are handling them in a way that you as the operator expect them to be handled.

An operator for the coordination, that's an aspect that many people think of network operation centers, network operating groups in North America, NANOG, and Asia APNIC. And they are throughout the world, but they are the means for the network operators to share information and talk with each other usually online, but by phone when need be. And they are what some people describe as the gurus that keeps the packets moving the way they're supposed to be moving.

And you need to know where your network operator group are, have contacts already established, and if something bad happens, you need to be able to react right then and know where and who to talk to. So the other fourth leg here is the MANRS project, which is a project that encourages a voluntary set of activities that are aimed specifically at the integrity and stability of the routing system. So those are kind of the operational aspects.

And now next slide, please. So the key takeaways from the documents is that I didn't make too strong of a point earlier, but I do want to say it now that there are incidents and routing anomalies that are occurring in the routing infrastructure hundreds of times a day, maybe even thousands. Nobody really knows, but there's a lot of them maybe the majority, I think a lot of people believe the majority of them are accidents.

Somebody did a fat finger entry of something, but others may be an intentional causing such as the Route53 Ethereum, MyEtherWallet attack. And as far as when you are watching and observing what's going on, in almost all cases, you can't tell a difference. So that's the reason for the SSAC121 describing these routing anomalies because we concluded that it wasn't worth trying to describe the difference and be able to say it because it really is visible outside of those that are actually affecting the activity.

So the Internet routing security, the next key point is that it's a combination of things. There are protocol security requirements. Those are important and very important. They need to be implemented and progressed, but so is having an accurate routing policy and a robust operational posture. So even if your operation is focused on something other than routing, you probably are going to at least make use of routing if you're a fair, even a medium sized operation. And you need to understand how the routing for your infrastructure is done and handled and where to go and what to do in case there's a problem with it.

And the third point is monitoring. And that's how you can detect if there is a problem with what you expect to be happening in your routing, but actually isn't. And if you don't know, such as the MyEtherWallet Route53, it was two hours before that was corrected. And it could have been even longer if there hadn't have been monitoring in place to flag that that is a problem.

And the fourth point is routing security is important, but it doesn't substitute for other important and critical security technologies, such as DNSSEC. It's a completely different aspect. There are times when one's security technology can help and sub provide alerts that you might not see otherwise when there's an attack on a different space in the protocol stack, but they aren't a substitute for each other. And just as the TLS is not a substitute or replacement for DNSSEC routing security and RPKI is not a replacement for DNSSEC or vice versa.

So you need to again, remember that security isn't one single bullet. You need to approach it holistically and think about it as a whole. Okay. That is the presentation. And I don't know if we want to take questions or not, Rod, or if there are questions I will let that be totally up to you.

ROD RASMUSSEN: Yeah. No. Let's go ahead and take questions by topic here. Do we have any questions for us on the routing work? I can see we have a question, Hafiz, please.

HAFIZ FAROOQ: Good morning, everyone. My name is Hafiz Farooq. I'm cybersecurity architect for Saudi Aramco. My question is about the routing security. As per my understanding, routing is not under the scope of ICANN. And this routing is directly threatening the DNS. So how we are handling the challenge of securing the routing itself? Because it is, at the end of the day, going to impact the DNS infrastructure. Thank you.

RUSS MUNDY: Yes. Thank you for that question. This is an interesting aspect that you flagged that routing as such is managed by network operators and infrastructure operators. It is different than the assignment of the number of resources. It is how they are actually used. And so routing is not really managed by any centralized entity beyond the operations that are making use of their assigned numbered resources. And so it is really at this point, I'm one of the reasons why the SSAC undertook this, is to produce a document that would provide helpful information to the broad community on how to improve the state of routing security.

Now one thing I did not mention earlier in running through the slides is the SSAC121 has a very extensive set of reference material. My personal opinion is it's the most extensive set of reference material on routing security that I know of in one place. So for more information and much more technical depth about some of our added security issues, the appendix of references in SSAC121 is an excellent place to go. And it really is educational, trying to get all of the operators that are involved in the routing system to do more and better security on an ongoing basis because, yes, it can affect certainly the DNS. It affects applications, it affects load balancers, lots of things.

ROD RASMUSSEN: Thank you Russ. Russ just to add a little bit of flavor to that as well and that as you mentioned, there's no central authority that really has, this is the remit. The SSAC itself commented on this, and we focused on its impact on the DNS system.

That said, we do have a broader remit. We're looking at all the identifiers and security impacts that can be felt in any part of the Internet for as an area we could comment on. In this particular instance, we didn't make any recommendations to the Board because ICANN, as you mentioned, doesn't have an actual ability to affect any kind of policy change here.

This is really about a couple of things as Russ just mentioned awareness. And we're playing together, trying to pull together a lot of useful information for people to take note of. And also to raise awareness in the DNS community particularly with some of the incidents that we've seen in the past. We had one example in there, but there's many others where DNS operations have been targeted by using the routing system. So that's why we put this out. So I see a nodding heads, so I think we're good. Yeah, a thumbs up. Any other questions?

RUSS MUNDY: We have one?

ROD RASMUSSEN: I'm seeing Leif.

LEIF SAWYER: Hi. Good morning. Leif Sawyer. I'm fellow. I just wanted to know if there's been any outreach done with like APRICOT, NPNOG, NANOG, ARIN, or any other local NOGS or RIR, LIRs to present this work and make sure that it's getting out to the people who are operationally responsible for the networks.

ROD RASMUSSEN: Good question. Not yet. But I think I mentioned earlier, we published this during the last ICANN meeting and one of the things we're thinking about and I'm going to try and coordinate is working with ICANN outreach to get the word out about this. Although, I do know that it has gotten some uptake in various places, but thank you for your point. I think if you publish something and you don't tell people it's been published, it's a bit of a challenge, but I think this is one of those papers. We really want to take advantage of the fact that we've got resources here in the community. And I see, Warren, you get your hand up.

WARREN KUMARI: Yeah. Thanks, Warren Kumari, SSAC. So, I mean, a fair bit of this work is actually a collection of work that has already been presented at places like APRICOT, RIPE and NANOG, etc. The primary thing that this does is it helps reframe it in a way that is suitable for the ICANN audience. So if it could be presented at those and possibly should be, but I think so that's main utility is helping people in the ICANN world and DNS operators understand stuff which people at NANOG and RIPE etc., already know.

UNKNOWN SPEAKER: And I'll just add that the APNIC chief engineer was one of the work party members and a key player in putting this document together.

ROD RASMUSSEN: Great questions, by the way. Thank you very much for that. Go ahead, Patrick.

PATRICK JONES: Patrick Jones invited participant from ICANN org. I just want to flag that we do have an event coming up in November that is coordinated by the ICANN Office of the CTO. It's called the DNS Symposium, and that might be a good opportunity for Russ or someone from SSAC to present this work to a technical audience.

ROD RASMUSSEN: Fabulous idea, Patrick. Let's talk about that after the session today.

KATHY SCHNITT: Rod, we have a question and chat. This is from Peter. Do any of SSAC's other documents include more examples of routing hijacks that affected the DNS.

RAM MOHAN: Thanks. This is Ram Mohan from the SSAC. Yes. We've covered this topic over the years. I don't recall the exact document numbers off the top of my head. But if you go navigate to our website, you can actually look by. We have the documents organized by categories as well. And you can look at the documents that focus on routing and hijacks. Thanks.

ROD RASMUSSEN: There we go. Any other questions before I move on? Okay. Thank you very much. A bunch of really good questions. I appreciate it. Next slide then, please. Okay. This is our next bit, the SAC120, Steve Sheng. I believe you were going to give us a rundown on that.

STEVE SHENG: Thank you, Rod. Good morning, everyone. I'm Steve Sheng. I'm the ICANNs org staff in support of this work party. So I presented on behalf of the work party. So this is SAC120. It's an input to the GNSO, IDN, EPDP on IDN variants. So let's start with some definitions here.

An IDN variant is in alternative code point or sequence code points, for example, in some scripts that could be substituted for a code point, or sequence of code points in a candidate label to create a variant label. Now sometimes the variant labels is considered the same some measure by a given community of Internet users. However, there's generally no agreement of what that sameness requires.

So just to pass this definition a bit, when it comes to the definition of variants, you can have a code point variants. That's what's defined here and is in scope for ICANN. And there's another aspect what we call a host string variance that is not in scope here. So for host string variants we're talking about, for example, transcriptions from the Greek script to Latin.

We're talking about linguistic variations, for example, like, in UK, color in the US, they spell differently. Encyclopedia, the AE versus EA. Those are not the type of variants we're talking about. We're focusing on code point variance. So I think in the in the SSAC world party, the point, the key point the SSAC wants to make is in the DNS two variants are two distinct domain names, is the users of those specific communities that will recognize variants as equivalent.

So next slide, please. So we're looking at the variant management issue, the SSAC, things that a variant management can really serve two purposes. The first purpose is to enhance the security and stability of IDNs that have variants. And the second purpose is to promote an acceptable user experience for those

IDNs that have variants. And from the SSAC's perspective, the first goal is the most important one.

Now how do we ensure security and stability of IDNs that have varying labels? Well, from the SSAC'S perspective, the IDN and its variants must be treated as a single package from a domain name provision and life cycle management perspective. So for example, when you register a domain name, the variant label set must be treated as a single package.

Management actions to any domain needs to apply for the whole package. So this includes takedowns, transfers. Without such rules, the users of IDNs, with variant labels will be susceptible to phishing and other kinds of impersonation attacks. So that's why from a security and stability perspective, they needs to be treated as a single package. Now to promote an acceptable user experience for IDNs that have variants, variants of IDN that are in actual use can be delegated.

However, next slide, please, the SSAC point out some very important limitations for the policymakers. The first limitation is when defining rules for delegations, the policy makers need to have in mind that there is no protocol solution. In DNS, or in any other protocols, for example, HTTP, SMPT for mail, to enforce equivalence of variants labels. And this is a very important limitation.

There has been past efforts in the ITF, but those have not gained traction. So that means there's no protocol solution. And the other very important limitation is in management of variant domains can introduce a combinatorial explosion for registries, registrars, and registrants that needs to be managed carefully.

So what do I mean by combinatorial explosion? So if you think of a, let's say, a Chinese script, a simplified Chinese script, a TLD with five Chinese characters at the top, and then the second level, you have three characters. If each of those characters have variant labels, it is a combination, the variant set gets very large as the label increases. So that produce operational issues for registries and registrars and needs to be managed very carefully, otherwise, it will cause issues. So I think because of these limitations from the SSAC'S perspective, the provisioning of variant TLDs and the management of it cause for a very conservative approach in the delegation and management of that.

So how do we define conservative? So, why don't you start with the question, is one label sufficient? If not one label is not sufficient, are two labels necessary? So then apply. There's a set of technically driven criteria to really limit the number of variant TLDs and labels activated in order to reduce these issues.

Another alternative approach for conservatism is to place a limit on the number of delegate labels. So for example, in the simplified and traditional script community, a registry can only activate a simplified label, a traditional label, and then a label of the registries choice. So at maximum three labels. So I think those are the rules can be in discussion, but the goal is to ensure conservatism. So I think that's the one key element of the SSAC advice.

And finally, I think last but not least, the root zone is a very special zone. Right? Because you're going up further up the DNS tree, the root zone is shared by everyone on the Internet. So then that means whether you're at ccTLD or your gTLD of that script and it needs a set of label generation rules to ensure minimal conflict, minimal risk to all users, and minimal potential for incompatible change over time. So in this regard, the SSAC recommends the root zone label generation rule developed by the multi stakeholder community should be used by ICANN to determine variants for all current and future TLD labels.

Now the label generation rule is on version 5. It includes 26 scripts. So I think the global multi stakeholder community spend a lot of time defining what code points can be included and what other associate labels, variance for those labels. So from the SSAC's perspective, that needs to be used to calculate variants for current and future TLDs. So I think that's a quick overview of

SAC120. This was again provided as an input to GNSO's IDN EPDP on IDN variants.

ROD RASMUSSEN: All right. Thank you, Steve, for running through that on behalf of the work party. Are there any questions from the audience? Oh, over here, please.

NABEEL YASIN: This is Nabeel Yasin, for the record. I am an ICANN75 panel. My question is regarding the technology. I mean, the Internet is based on, let us say, not all technologies is stable technologies, but when they were invented, there was no security, no big routing issues and so on. And now some maybe telecom companies, huge telecom companies or countries is trying to reinvent the Internet again with new protocols, and there are some proposals like the new IPs or maybe other things. So how the SSAC is dealing with such challenges? Thank you very much.

ROD RASMUSSEN: Okay. Yeah. It's not quite on topic here. And actually, one of our current work parties is looking at some of those issues I think you're talking about. So let me defer that question and we've got a work party on the evolution of DNS resolution, which touches, I think, on some of what you're asking about. So why don't you look at that presentation? And then if that doesn't help with your question, we'll come back to that. Cool. Hafiz, you have a question.

HAFIZ FAROOQ: Yes. I have the question about LGR version 5. So as you said, it is right now covering around 26 languages. And definitely, there are many more languages around the globe, which are rightly spoken by different communities. So are we going to expand it? And what is the timeline for that?

STEVE SHENG: Thanks. First of all, clarification. LGR for the root cover only scripts because in the root, there's no linguistic context. So for example, for given LGR, let's say, the label generation for the Arabic script, so experts needs to, from a variety of languages that use the Arabic script, get together. So this includes Urdu, Farsi, the Arabic language, and even the Arabic speakers in the northern Africa. So those are the global experts come together to develop the script tables for the LGRs.

As you said, currently, there are 26 scripts. I think the last time I checked was really is incumbent upon the Internet user community to come together to form what we call these labeled generation panels that with the support of ICANN to develop the script tables for that. So if there's not enough interest, then the LGR generation panel cannot be seated. So therefore, those cannot be developed. So again, it's really a call to the community that use those scripts, needs to get together to develop those generation rules. Thanks.

KATHY SCHNITT: Sorry, Rod. John Levine is online. He wants to make a comment.

ROD RASMUSSEN: Very quickly. I just realized we only have 10 minutes left in the session. We got a lot of stuff we wanted to cover. This has been such a good discussion. I hadn't realized the time has gone by. John, very quickly.

JOGN LEVINE: I can be quick. I thank Steve for his excellent summary of the situation. I'm drawing attention to, usually, that there is no protocol solution for web or mail or anything else. This is a topic we've been going around for a decade. And although it is fairly straightforward to imagine ways that we might do web and mail, automatic configuration to variance. Nobody has ever done it, which tells me that there actually isn't a lot of interest in configuring variants.

So I think while it is important to look at the security issues to make sure that we don't inadvertently provision variance that might be confused with each other, the main thing is simply to basically block variance that might be confusing, whereas in reality, as soon as people provision one variant, they are done. So I think that's somewhat simplifies the problem space.

ROD RASMUSSEN: Thank you, John. I'm going to move it over to NCAP. Matt do you want to go a quick run through? We've had two sessions, I believe, on this already. So we can quickly run through that.

MATT THOMAS: Yes. Thanks, Rod. This is Matt Thomas. I'm one of the co-chairs with Jim Galvin on NCAP, the Name Collision Analysis Project. I'm just going to briefly run through this, like Rod said, since we've already given a full preliminary session on this. ICANN ask SSAC to provide some advice on the strings of .home, .corp and .mail as well as answering nine questions specifically related to name collisions. And that's what the NCAP discussion group has been focused on over the last couple of years. There's 25 members, 14 SSAC members, and 23 community observers currently engaged in the efforts to do that.

Next slide, please. Two of the most recent publications that have come out of the NCAP discussion group are, one a case study of collision strengths, and this was specifically looking at a longitudinal analysis of .corp, .home, and .mail, as well as three additional strings that we've pulled it in .internal, .LAN and .local using DNS telemetry data from A and J root servers. That case study really highlighted the evolution of the DNS queries for those strings over time and showed the heightened elevations of named collisions persisting in those strings.

The second was the prospective study that looked at the ability to observe and use telemetry data within the DNS hierarchy system for named collision risk assessments and to understand the particular guardrails when looking at DNS data at particular points in the DNS hierarchy in terms of what and how it can be assessed and what kind of guardrails it needs to have with that assessment.

Next slide, please. So some of the key findings. I think the main one I want to say here is that name collisions are and they'll continue to be an increasingly difficult problem. This was clearly demonstrated within the case study. We also observed in the case study that some of the underlying root causes of those name collisions are the same things that were identified in 2012, which are DNS service discovery protocols and suffix search list processing.

Within that case study, we also have termed something that we've called critical diagnostic measurements, and this is a set of quantitative measurements that look at telemetry data to better assess the impact or risk associated with a named collision. And those CDMs or the critical diagnostic measurements are pretty much the fundamentals that were taken from 2012, codified a little bit more here and that NCAP discussion group and aren't going to be used going forward as our a recommendation into the development of our workflow in terms of how named collisions can be assessed in a sustainable, repeatable fashion. And to that point, we've also identified that there might be some opportunities to extend existing measurement platforms to help inform applicants around existing name collision risk prior to their application.

Next slide, please. So at a high level, these CDMs are critical diagnostic measurements really focused on some of the items listed here on the slide. They start out with query volume, but volume in itself is not a definitive end all be all kind of measurement describing the risk of a particular string. Just because something has high volume doesn't mean it's particularly risky.

There's also other attributes and measurements that need to be considered. And those need to be measured over different vectors, including diversity. And diversity is then spread over multiple different dimensions, including query origin diversity. Is it coming from multiple IP addresses, multiple different ASNs? What is the Q type diversity, the query type diversity, what is the diversity of the labels, the second label domains, so forth, and so on.

And those quantitative measurements help establish a profile for assessing risk. But, obviously, there is also a more qualitative assessment of what needs to be done on a named collision strengths, and that's a little bit more bespoke on each individual stream. But collectively, what these types of measurements are designed to do or intended to do is to help inform the potential assessment of risk for Impact or harm by assessing those over all of those different dimensions.

Next slide, please. So the main object of the NCAP work is to develop a framework to create a sustainable, repeatable model for assessing a name collisions strengths going forward and also provide some guidance on the existence of named collisions. We are in the hopefully the home stretch of writing the Study 2 report going out and we are targeting the fourth quarter for 2022 for its release to public comment. Next slide, please. If you are at all interested in contributing or learning more, here's the information for joining the discussion group, please come all voices are welcome. Thank you.

ROD RASMUSSEN: Thanks, Matt. I'm going to skip questions on this since we've had a couple of sessions publicly already. Please feel free to send the questions in if you have them to the NCAP discussion group, which can be found from the ICANN website. But next slide, please. So here are the current work parties we have going. We only have a few minutes left, so I want to go through this very quickly. We're talking about NCAP. We got two that we'll touch on a minute each here. So Peter, could you please take the next slide on DS Automation Work Party.

PETER THOMASSEN: Yeah. Hello, Peter Thomassen, SSAC. So I'll try to make it quick. The way that DNSSEC chain of trust works is that in the child domain, some second level domain, for example, you have DNSSEC keys. And to establish that those are part of the chain of trust, you have to somehow link them in the parent domain that's done by adding cryptographic hashes with the keys in the parent domain in so called DS records, and those live next to the NS litigation records.

And then the way to deploy those today is usually the manual process or often a manual process that involves the registrant, and the registrar, and the registry, and also the DNS provider who has the key authority and the registrant has to fetch that information from the operator or the DNS provider. And then some are pushed upwards. And it's complicated. There's different approaches of doing this and often it doesn't happen. So there seems to be need for automation for this, and this is what the work party is dealing with.

The intended audience of the document the work party is going to produce are the registry, registrar, and DNS service provider industries, and we are investigating in the work party. What is the current state of how DS records and the parent are managed? So we have a survey on that, and then based on that, we intend to describe the current set of things, the options that are available, and possibly recommend specific methods that can increase the level of automation so that when more automation is deployed, it will be easier to secure delegations within a SSAC and increase the security delegations rate.

ROD RASMUSSEN: Well, thank you, Peter. We're going to move on in the interest time because we're right up the end of the session. And please go to the next slide. I'll quickly talk about this because I hope answers your questioning asked earlier. So the evolution of DNS resolution, we have a work party that is looking at new technologies, new protocols, etc., and new operational parameter or operational methodologies that are affecting the resolution of DNS out there.

And we're taking a look at this from a fairly broad perspective because it affects every player in the ecosystem from the authoritative side to the resolution side, etc., and how users interact with the DNS. Because the resolution of the DNS is how you actually get from point A to point B. The publication just tells you what prints out, resolution reads them out for you, so to speak.

And we're looking at that, and you can see from the scope here, we're actually looking at things like new alternative naming technologies, etc. They've been very much in the discussion lately as part of that work. We're looking, this one's probably going to be next summer or sometime in the fall, even next year. There's a lot of work we're doing here, but this is addressing exactly these emerging technologies, etc., that are affecting things in this community that are happening elsewhere.

So it was inspired a bit by our work on DOE and DOT, which I don't remember. What's the DOE/DOT stack number report? I don’t remember off the top of my head, but we did a report on that fairly recently that was kind of a precursor to this work. So that's that one.

Next slide, please. New work that we're looking at potentially. SSR datasets, and these have not changed since our last meeting, but there's some interesting topics there as you can see. I also will point out that on the prior slide about current work is the DNSSEC workshops, which are this afternoon here in Kuala Lumpur. So I'm going to wind down this bit. If you see the next slide, it's about outreach, etc., which we don't have time for right now.

However, if you're interested in learning more about during the SSAC, we are on our new recruiting period, which will go for the next few months and you can contact myself or Julie, and our support staff, you can see the address there. These slides will be available. And I know there's at least one question out there of a general nature that I wanted to take. I believe it was George, you are very patient, and I appreciate that. And I'm sorry for running long. It was a really good discussion here today and lost track of time. So George, please.

GEORGE KIRIKOS: Hi. George Kirikos for the transcript. Yes, I wanted to draw attention of effect to the transfer policy working group. They issued a report recently and SSAC made a brief comment pointing out the DNSSEC issues. However, there are much bigger security issues in that report that affect registrants. So I would hope that this is a topic that you would put on your agenda as possibly new work, in particular, past SSAC advice or insights that to treat transfer attempts as a security event to check and recheck.

And this working group is proposing the actual removal of a very important security measure, which is what's called the losing FOA, which briefly, when there's a pending transfer request at present, the losing registrar will send a confirmation request to the registrant who has an opportunity to either ac or in-ac. I accept or reject the pending transfer.

And the working group is actually proposing to remove that important security safeguard. And so that's one of the things I discuss at length in my comments submission and in piece of the URL into the chat room. Just looking at it, more broadly, I think the security could be enhanced greatly if we moved instead of the current security architecture.

If transfers were re-architectured to have more of a push structure, kind of like wire transfers. Because right now, everything kind of relies on the security of a secret, namely Auth-Info Code, which they're planning to rename as the transfer authorization code, TAC stack.

That has very inherent weaknesses in its design and if we reexamined how transfers are structured, that could entirely be eliminated and be more like a wire transfer where you don't rely on a secret. You actually can publicly post the address at which you receive a wire transfer, and I have to worry about that being stolen by malicious parties. And I know time is running out, so I just want to bring out your attention. And if anybody wants to read my comments, they're in the chat room link or go to my blog. And hopefully this is an issue that is of concern to some of your members and hopefully the entire SSAC. Thank you.

ROD RASMUSSEN: Thank you very much, George. I really appreciate the questions, very topical. I believe Steve Crocker may have a quick response as he's been part of that work, if I remember right. Steve, you want to just 30 seconds and then we got to wrap up here in the room because we're getting a kicked out by the ccNSO.

GEORGE CROCKER: Thank you, Rod. Thank you, George. Appreciate the comment. I've been the official SSAC person on there, although the peculiarities of the arrangement are a little interesting. As you pointed out, the focus that I brought there was the DNSSEC issue. And I want to note that Jim Galvin has also been participating I think from the registry community.

My assessment was that they had the other aspects of security fairly well under control. You're raising the point that they may not. And so I simply want to say, listening to you, take note of it, it would take note of it, and I personally and I hope others, including Jim, will look into it. We can't say anything more about it at the time, but thank you for the comment.

ROD RASMUSSEN: Great. Thanks, Steve. I really appreciate that. Yeah. We'll take that on our board. I know we've had some discussions around this topic, but hadn't raised to the level of doing work on it. So we'll definitely take a look at that. We have a workshop coming up later this fall. We really have to go. Okay. So we're safe for the moment, apparently. That said, are we okay with ICANN staff staying in a few more minutes? Because there's a couple more questions in here.

KATHY SCHNITT: We're okay.

ROD RASMUSSEN: Okay. So I thank you. I appreciate that on the staff part to really very much. I believe. George, did you want to quickly respond. I think I see your hand up, and I want to move on to the next topic. If you give quick respond, please do.

GEORGE: Yes, Please. Thank you. A quick question about the transfer policy working group. This group is focusing on lockdown period. And I have established an estimated block period for transfer DNS names. I wonder if it's possible to avoid this. I wonder if this lockdown period is useful. And it is possible to avoid this lock period by using some other security mechanisms since it will be very helpful to make a period limited to some of the operation and financing transaction. Thank you.

ROD RASMUSSEN: Okay. Thank you for that comment. Steve, did you want to add any more to that? No, okay. Thanks. We'll take that one. Thank you for your comment. We'll take that one on our board as well. Then we have, okay, George, did you want to go ahead and respond real quick? And then I'm going to cut the queue off after Gabriel. George?

GEORGE KIRIKOS: Thanks. George Kirikos, again for the transcript. I just want to thank Steve for taking a look at it. I know Jim Galvin is on that working group, although he's made some mistakes, not recognizing exactly what the working group has proposed. I pointed that out in a recent blog post. He thought that a certain mechanism was still in place and had to be corrected. So I think they're kind of rushing through the comment review and not necessarily taking their time to really seriously consider all the concerns that have been raised by the public and hopefully the effect can add some gravitas to the concerns if they obviously agree with us. Thank you.

ROD RASMUSSEN: Thank you for replying. We have gravitas. Okay, our last question, I'm sorry, I do have to cut off the queue, is Gabriel, please.

GABRIEL KARSAN: Good morning. My name is Gabriel Karsan from Tanzania, an ICANN fellow. My question is more rather on the evolution of the DNS. Right now, we're going with emerging technologies such as encryptions, quantum computing, and software based [01:07:35 - inaudible].

So I think it poses a big threat where it's very easy to break the Internet with this technology if they're given to rather communities with malicious intent, and we see the evolution of technology of malwares driven by AI just like the Log4j. So how is SSAC prepared in first raising capacity and equipping resources to the normal Internet users and rather civil society in mitigating these errors? Thank you.

ROD RASMUSSEN: Thanks. Good questions. I'll give one example on the first part you mentioned was quantum computing. SSAC actually did provide a comment on when more recent nest rounds of for comment, around the pointing out that the DNS has this, in particular, DNSSEC, is reliant upon cryptography that will be broken at some point. And that when NIST is considering candidates for algorithms, for post quantum computing, that they should take into consideration the needs of the DNS for giving us the capacity for messages, etc. flying around in the DNS.

So that's an example of an area we actually have recently made a comment. I don't remember the number of the document, 106? SSAC 106 actually talks exactly the issue you just brought up. Oh, 107. Okay, there we go. If you go to the website where ICANN has a thing, you'll see that report. And that's something we will be probably keeping tabs on moving forward. And if there's issues with, as the technologies come out as it may, if you've been paying attention some of the candidate cryptography has already been broken. So it's ever changing field.

So I'm going to wind down the session right now. There is a plenary on fragmentation that our members, several of our members are very keen on attending. It was coming up soon. And let me put another plug in again for the DNSSEC workshops. I believe they're in this room. Are they not, Kathy?

KATHY SCHNITT: No. It's actually conference room 1. Thank you, Rod.

ROD RASMUSSEN: Oh, conference room one. Yeah, the conference room one this afternoon. And some of these very topics that we didn't get time to talk to today may very well be covered in that session or other really interesting technical, geeky stuff, which I'm glad to see this room full of likeminded individuals. So thank you very much for being here and taking your time and asking very thoughtful questions today. Very much appreciated. I will be here for a few minutes long with Julie and a couple of us if you want to come up and have a quick word with us before we all go off to that panel. Thank you very much. With that, I'm going to close the session. Thanks.

KATHY SCHNITT: You may stop the recording.

[END OF TRANSCRIPTION]