BUENOS AIRES – SSAC Public Meeting
Thursday, June 25, 2015 – 08:00 to 09:00
ICANN – Buenos Aires, Argentina

PATRIK FALSTROM: …the contract between NTIA and ICANN regarding IANA, and then SAC 69 which is the SSAC recommendations to the operational communities, and specifically the names community, on what they should include in their proposal that they are submitting to the ICG.

SAC 70 is an advisory on the use of static TLD and public suffix list was released 29th of May. Then we have SAC 71 that is the comments on the CCWG from SSAC that we released on 8th of June. So that was the first open consultation that the CCWG was running.

Then yesterday we released SAC 72, which is the SSAC evaluation of the CWG stewardship or the CWG names proposal. The SAC 72 is an evaluation of the CWG proposal – is an evaluation according to SAC 69. So what we did was that we took the proposal, CWG names, we took SAC 69 and then we simply compared whether the proposal is fulfilling or our requirements. And the result of that is that we adopt – we approve the CWG names proposal and that was something we did yesterday. Next slide, please. Next. And this I already described. Next.

If you look at where we are regarding milestones, we had DNSSEC workshop at ICANN 53 yesterday. We released SAC 70, 71, and also 72. We have our plan for the third quarter to give advice on the registrant protection and credential management. We'll talk a little bit about that later.

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

In the fourth quarter, to be ready with advice around new gTLD program review, and also have a DNSSEC workshop at ICANN 54. Next.

So advisory on public suffix list. But before that, let me ask if anyone has any questions, just because we're sitting in a fridge and people want to leave.

So SAC 70 public suffix list. Next slide, please.

Public suffix is something that tried to – is a domain under which multiple parties can register domain names. If we look at, for example, how it was historically in the U.K., people register under co.uk, not under uk, etc. There is no programmatic way to know where the actual zone card is, or even if there is a zone card, where it's possible to register domain names.

Tracking these boundaries a little bit, that is a little bit tricky, but there is an interest of checking the boundary for various different kinds of things. For example, for certificates, for cookies, and other kinds of things. So you don't want, for example, to in the browser to be able to set a cookie for a complete top-level domain or for the whole domain where people can do registrations. Next slide, please.

To be able to know where this zone card is or where these administrative boundaries are, there is something called public suffix list created. And that is configuration information that informs, for example, browsers on where these boundaries are.

So what we were looking at in SSAC is that we were looking at, for example, what these suffix lists are used for, and we do see, among other things, that they're used for cookie settings, as a sales certificate, navigability, TLD validation, domain highlighting in the browser, and a few other kind of things.

There are multiple of these public suffix lists and they include slightly different information. They have different syntax and the browsers are using these in different ways.

So, you see, this is just a few examples of the use-case description and what applications are using this feature. So you see there is also a difference between the different browsers, for example. Next slide, please.

An example is that when a user in the only one input window in Google Chrome enter [nice.allfinance], in that case, you actually end up on that webpage. Well, if you type it in Apple Safari, then both of these are current versions. If you type it into Apple Safari, Safari don't understand that it is a domain name and sends the user to the Google search page This is just one example of different result when the same input is given in the two browsers. Next slide, please.

So what we found is that there is inconsistency and also compromise between the convenience of use and [inaudible] contents. There is no consensus definition of what public suffix list is, what it actually should contain, how people should use that data, etc.

It's also the case that we see a lack of accountability mechanisms to ensuring that PSLs are produced in a consistent, fair, and unbiased manner and it's also the case that there is a knowledge gap between registries and others that set the policy that is expressed in the public suffix lists. And because of that, because end users, applications use different public suffix lists and in different ways the end user result is not really harmonized and creates surprise.

On top of that, or one of the reasons might be that there's no universal library, or framework, or tool. Each developer and programmer is implementing the use of PSLs in whatever way they want themselves. Next, please.

It's also the case that even though people know that public suffix lists exist and a change in policy is to be implemented, there's also a great difference in what time it takes to get that policy change, for example, implemented and distributed using the different public suffix lists.

Even though the [Mozilla] public suffix list is the most dominant one that most people use, there are a multitude of others and that is something that is also creating a little bit of a problem.

On the other hand, there is also reason why there are multiple public suffix lists, because they are used for different things. So it may be difficult to actually create a one-size-fits all public suffix lists for all audiences covering any applications and uses. On the other hand, there is a lot of data that actually is shared and is the same or supposed to be the same in all public suffix lists Next slide, please.

So we have a couple of recommendations. They include, of course, a lot of development activities. We recommend that IETF should standardize PSL alternatives and the [inaudible] Working Group, for example, is looking into these things.

It would also be good if people actually agree on what is meant by public suffix lists and other terminology that is used around these issues.

We do believe that ICANN and the [Mozilla] Foundation can do better job on informing, for example, TLDs and others that are described in public suffix list on the existence of public suffix list and how to make changes.

We also believe that ICANN could encourage the software develop community to develop and distribute programming and operating system libraries for PSLs. [inaudible] see this as part of collaboration that we would like to see between ICANN and the [Mozilla] Foundation on simply getting a much better environment for the developers, the software, and the developers of policies around what is described in pubic suffix lists. Next slide, please.

We also hope and encourage application developers to do simple things like, for example, agreeing on a [inaudible] file format and some modern authentication protocols so people can actually validate that their public suffix list is the one that is intended to be used.

We proposed that IANA should host a public suffix list that contains information about the domains that IANA have direct contact with because IANA is really the registry for TLDs and for the basic minimal information that IANA is collecting. They could as well run the public suffix list with that information that, if interested, other public suffix lists could bootstrap their work and their lists with the information from IANA as a way of getting at least some information be the same all across the various public suffix lists that exist in the world.

It's also the case that we think ICANN should explicitly include the use and actions related to public suffix lists as part of the work that ICANN already is doing related to universal acceptance, because even though public suffix lists is by far not the only issue with universal acceptance, it is a piece in the puzzle that needs to be taken seriously. Next slide, please. Is there any questions on public suffix lists?

Okay. Next document, SAC 71. Next slide, please.

Once again, the SSAC charter says that SSAC advice [inaudible] ICANN community and board on matters related to the security and integrity of the Internet's naming and address allocation systems.

That is what we are chartered to do and we have had quite a large number of discussions within SSAC and also with ICANN board and others on how to interpret this charter.

We have found that, for example, there are two things which are not in scope. The first one is that we are not, for example, making any advice or overlooking ICANN's own IT systems. We are looking only at the naming and address allocation systems. Of course for them to work it might be the case that ICANN or other organizations that manage these identifiers do it in a certain way and it might be the case that we are investigating because of that reason what ICANN and other organizations do.

But we have a good relationship with ICANN IT and security team, but we are definitely not overlapping. We have discussions every meeting with them to make sure that we're not walking on each other, stomping on each other's feet.

The second important thing is that SSAC has not been given and we have not sought any [inaudible] for the advice other than that we try to create advice of very high quality.

We also think that it's a good thing that whoever we recommend do things that they evaluate the recommendation of ours based on the quality of our report, so that whoever we recommend do things that they have the ability of, to put it bluntly, ignore what we are saying. We see that as a strength. It forces us to write good reports, come with precise recommendations, explain why it's important to follow the recommendation, and that is also how we also measure our result. We are keeping track of how people reference our recommendations. We are specifically together with ICANN and ICANN board working on tracking specifically the advice that we are giving to ICANN board. Next slide, please.

Because of the charter, we don't really work with organizational structure or architecture or those kinds of things. We simply cannot comment at this point in time on the legal structure that might be needed for ICANN. We are a little bit concerned also that the proposed [Membership Model] that was proposed in at least what the CCWG was talking about like a week ago or two, a little bit nervous that if it is the case that if it is imposed on us, that it might change the way we operate and we need to reform ourselves. Next slide, please.

As a follow up to us being nervous, of us being forced to do work in a different way, we do expect and hope that the community will at the end of the day choose a structure for ICANN and us and otherwise that recognize the role and importance of expert advice on security and stability.

It is also the case that the bylaws of today include as the first bullet the importance of security and stability issues. It is proposed is to be that that point is to be a commitment in the Articles of Association. We do see a trace of that being important in those sort of nice texts, but it's also important that is followed up by an organizational structure of ICANN as a whole that actually makes it possible for ICANN to live up to those goals. It's nice to have a mission for an organization, but it's also pretty damn good to be able to deliver.

Then we just reserve the right to make additional comments in the future if it is the case that we find that being needed. Next slide, please.

Is there any questions on that? We don't have any slides on SAC 72, but we are happy to answer questions on SAC 72 as well. Okay. Ben, do you want to do this? I think it's much better if you do it than I do it. Sorry, we do have a work party on registrant protection and credential management, and Ben Butler and Marika Koning are the ones that are leading that work. We have other SSAC members being active. And just because Ben happens to be here, I hand it over to you, please.

BEN BUTLER: Good morning. Apologies on behalf of Marika Koning who could not be at this meeting. What we are working on right now is a follow up to some previous recommendations made in past SSAC documents, specifically SAC 40 and 44 trying to identify best practices around protecting registrant data and credentials as they log into manage their domains.

We feel that there has been a persistent increase in the negative consequences of poor credential management in the registrant, registrar, and registree authentication space. So we felt it was an opportune time to present more specific, more targeted, and more operational recommendations that would help to the registrant, registrar, and registree communities to better secure the potentially valuable assets that are their domain names.

We have been working rather quickly to try and get this information published because we recognize the need for it within these communities. We are working very closely currently with the registrar and registry stakeholder groups, so that as we identify common practices in play now that we are representing a consensus view of what people are actually doing that will help us to identify the shortcomings or the shortfalls of things that could be done relatively easily and will give us the biggest impact in the domain name space to help protect against domain name hijackings in the form of unauthorized transfers between registrars as well as other problems that we're seeing like malicious A records being created within the customer account.

UNIDENTIFIED MALE: We do have more slides. We just realized you're not saying, "Next slide, please."

BEN BUTLER: I didn't realize we had slides. I apologize for my lack of informed nature. That was a very impressive deduction. Next slide, please.

Okay. So we're going to be able to blow through these slides relatively quickly. As I said, we're augmenting the previous slides. Our target audience is the wider ICANN communities – registrars, registries, registrants. Everyone and the kitchen sink essentially within this name space. Next slide, please.

We will address credential lifecycle in its entirely. The distributing, storing, renewing, revoking, and recovering name credentials as well as transfers. We feel what is within scope of this document is potentially all credentials used to authenticate an identity of a registrant or a registrar or a registry. Those relationships between the three Rs, as some of us call them, can get very complicated depending on the particular TLD and registrar and registry involved. So we're trying to be sensitive to all that confusion.

We're also trying to include any relevant policy issues that can support or hinder credential management in general in this space. Next slide, please.

As I mentioned, we feel that the problem is that there have been numerous recent attacks, compromises of high profile domains that we've all been seeing in the past 18 months to two years in particular. And as recently as probably last night, I didn't do a particular search for the information, but they're ongoing.

We want to look at credential use. How are they being used? What things are being used to validate people's identities and how we can do better at it.

We want to create a practical checklist so that operational teams within registrars and registries can go down the list and see where there are things that they can do better. Next slide, please.

We began this work in Q1 and Q2. We developed initial drafts. We began consulting with the larger registrar and registry community at ICANN 52, and again at this ICANN 53 meeting. It is our intention to develop a final draft and publish a document well in advance of the Dublin meeting. So stay tuned for that. Next slide, please.

What we're specifically asking for right now is sections four and five of our document, the use of credentials and how the current credential life cycle management takes place within the registrar and registry community. We've asked specific questions on issues and problems people have encountered with some of the basic security counter measures that they might be able to employ, such as multi-factor authentication, backup and storage of credentials, distribution and that sort of thing.

We also want to try and identify areas where there might be tools or software development that would aid in the credential security and management areas, so that the operationalizing of our recommendations can be more easily applied.

We want to make sure that we're being sensitive to solutions that are scalable both for small registrars as well as large registrars and registries. Next slide, please.

And back to Patrik. Oh, questions, sorry. Any questions? Back there?

CRISTIAN HESSELMAN: Hi, my name is Cristian Hesselman I'm with SIDN dot-nl registry. Perhaps it's out of scope, but are you guys also considering information exchange between registries and registrars? For example, when a registrar gets hacked.

BEN BUTLER: Yes. That is absolutely within scope.

CRISTIAN HESSELMAN: Okay, all right. That's cool. Thank you.

BEN BUTLER: [Steve], right behind you.

WENDY SELTZER: Thanks, Wendy Seltzer, W3C. I'd be interested in seeing what you're working on to the extent that these are web- based credentials. We at W3C have some work getting started around web authentication and improving that beyond the user name and password to factor authentication; multi-factor.

BEN BUTLER: Excellent, thank you.

PATRICK JONES: Just a brief mention that SSAC also submitted a workshop proposal for the Internet Governance Forum in November around this topic and it was accepted. So the document will probably be of use to the IGF participants for that meeting, too.

BEN BUTLER: Yes. And I think I'll take the liberty of speaking for [America]. I believe she will be at that meeting to help go over our findings at that point. Any other questions, comments, snide remarks, general insults? Thank you. Back to you, Patrik.

PATRIK FALSTROM: Thank you very much, Ben. So the last portion of our meeting, just like we normally do, is that we talk about how we interact. Next, please.

The normal questions that we get this week just like others, people are asking what we're doing, why we're doing it, how do we prioritize, etc.

The new work that we are prioritizing is based on basically what we think is the most important at the moment. This week we have been discussing creating one or two new work parties. And what has happened this week is that we've been trying to talk with the community and hear what they think is important.

The two areas that we are looking at at the moment, one is related to CPs and quality or low quality of software in CPs. The other one we're looking at is misuse of IPv4 address space. Or more specifically, that people use IP address space that is allocated for other parties, but not announced by the address space holder.

Any kind of input we would like to hear from the community, what you want SSAC to work on and look at. I got a question just before this SSAC meeting, whether SSAC is going to look into the output from the label generation panels for IDNs. There are certain issues related specifically to a high risk for a [inaudible] explosion or variance to be allocated in the name space. And the question is whether SSAC is going to look into that. So those kind of questions and that kind of input from the community is very valuable when we are doing the prioritization. But the prioritization is something that SSAC members do internally.

One could say that we vote, even though we are not doing voting. We are tracking the board's response by following how the board has taken our advice into account and how that is implemented. We have tried to use one issue tracker that we have been using together with ALAC. It was a little bit troublesome to use that. And on top of that, we started to use the tracker without really knowing what process we are going to use for the advice.

So what we have done together with ICANN lately is that we have been working on actually looking at the process for how ICANN receives our advice. And as a second step, we are looking into better ways than Excel sheets to keep track of that process.

The process itself is almost ready and defined, and that's a very important step for us, specifically given the suggestions in, for example, the CCWG accountability to implement the ATRT 2 recommendation that ICANN board must take formal advice from the advisory communities into account.

The way we inform the community of its work is by, of course, publishing the recommendations. We publish the presentation that you just saw with our milestones, the current activities, and also by having these meetings.

We also meet other groups in the ICANN community during the meeting week of ICANN and answer whatever questions they have and also inform them of the work that we do.

It's also the case that this week we met with the ICANN board. It's something we have not done for a while, and that is something that we from SSAC side found being very useful. We are still to sit down together with [inaudible] to the ICANN board and see how to make those meetings even more effective. Next slide, please.

Questions that we would like to ask the community that we would like to get feedback on, and we have started to get some feedback because we are repeating these questions so people actually start to answer them, which is good.

We would like to know how people feel the documents are written. Are they well written? Are they hard to understand? If you are the target of a recommendation, do you think the recommendations are clear? If you are not the target of a recommendation, do you understand what is expected of the recommendation of the organization we asked to do something? Is the level of detail correct? Do you understand the findings? Should we expand more on the details? Do we write too much text?

We have got extremely good feedback on, for example, SAC 50 that I think was two pages of real document and then a preamble. Everyone really liked that document, but of course it's also – first of all, it's really hard work to write a short document as we all know. But on top of that, there's also risk that we take for granted that the reader do understand the context within which we are doing our work.

We also would like to get feedback whether you believe that the publications reach the audience, and for this public suffix list, we are now, for example, go into the IGF and having a meeting and try to do an outreach there.

I would also like to say I appreciate the feedback from W3C and we should absolutely see what we can do regarding public suffix list issues, but also the credential management issues and how we could do more – increase the quality, but also get better feedback on those documents [inaudible] work more on that.

We also don't mind, of course, feedback on what we can do differently to help you better, because the whole goal, our charter, is to give advice and help you in the community.

And then the last thing, of course, is to get to know what is missing from the list of work parties. We do have the ability to produce between four and eight documents a year, and the question of course is what should we do the next year? What is important? It takes about half-a-year to produce eight documents. Some work parties take a longer time, some shorter. But I would say half a year of effective time and then of course it takes a while to start the work itself. Next slide, please.

Please, Dan?

DAN YORK: Dan York, Internet Society. Two comments. One was on the CPE work that you're doing, or that you're looking at doing, is that to understand – I guess I'm just curious more about what are you looking at in terms of is that around DNS resolvers on the environments? What are you trying to do?

PATRIK FALSTROM: We don't know. That's part of the whole work.

DAN YORK: Okay, that's fair.

PATRIK FALSTROM: Okay. Warren is the one that should answer this question, but in general, I think the finding is that we think that many of the CPs actually suck and because of that, we try to see whether we could do something, or recommend people to do something, whoever we are going to say, whatever we ask them to do, to decrease the amount of suckery. It's that easy. Warren?

WARREN KUMARI: Yeah, what he said. I think [inaudible] just to raise awareness of the issues, understand the issues, see if there's any way that we can change the landscape so that it becomes easier for people and attractive for people to make CP that sucks less.

PATRIK FALSTROM: But to be clear, this is exactly the kind of feedback we want because these are work parties that have not started yet. One question I ask as the chair as sort of a measurement whether we should start a work party is basically to ask whoever wants to do work. I asked Warren in this case, which at the moment, he's holding the flag. It might wander around. We'll see what happens. I asked Warren, "So to be able to start the work party, can you just come up with some kind of idea on what we should ask whom to reach what affect?" And if that question cannot really be answered, the question is whether we should do something.

Of course we can publish a document just saying, "Oh, run for the hills! The world is crashing!" But it's much more effective if we actually can give advice that has some impact.

WARREN KUMARI: Well, yeah. I guess part of my suggestion around that would be we see a real issue with CPEs that have imbedded DNS resolvers, and one of the challenges we've seen from the DNSSEC space is certainly getting those things to turn on validation or to have validation in general. The next part of that of course is having validation and having updated validation with new algorithms.

I think the degree to which – I think the biggest problem with CPEs is people buy them from their local electronics store, put them into their – or get them from their ISP and they never update them, they never do anything like that and they just sit there for years until they get to be old and decrepit.

Anyway, second point, though, Patrik, on a suggestion around a topic was we had a discussion yesterday in the DNSSEC workshop around this whole area around upgrading new algorithms within DNSSEC. Specifically, we're looking at [ECDSA] and the places that that touches all across the environment, ranging from validators that need to updated, but also authoritative software. Registrars need to update their GUIs for accepting DS records and things like that. Registries need to agree to accept DS records and new algorithms. There's a number of different pieces like this.

Russ Housley brought up that the IAB has a document that's in the end of its process – it's going towards last call – around crypto-agility. It would be I think an interesting piece of work for SSAC to look at the idea of what would it take to – or what are the processes that need to be dealt with within the larger DNS community to upgrade the cryptographic capabilities within the whole environment. Specifically for DNSSEC, in this case, but in general.

Part of why this comes into is, again, just for the efficiency of the system, better security, smaller packet sizes, all of the pieces that fit in there. But I would suggest as a possible topic of work.

PATRIK FALSTROM: Thank you. Any SSAC member want to comment on that? If not, I'm going to just say thank you very much for that input.

[ED LEWIS]: Actually, I was debating saying the same thing Dan did. That situation he was talking about I've seen in looking at universal acceptance last year where the problem came down to being able to enter in identifiers in the new TLD program.

I see a general problem with user interfaces restricting what input they allow in and that hinders our ability to either add more TLDs, add more identifiers out there, add protocols, [use] some of the other technologies out there. I think that's a wider problem than just the DNSSEC and the crypto-agility. It's a widespread problem with user interfaces that we really haven't addressed. Contact management systems I think was what I was tracking down.

Those developers are the ones that need to be informed that there's less need for certain types of [type checking] they've been doing. I think it's overly aggressive.

PATRIK FALSTROM: Thank you very much for that. One thing that we are of course looking at before we decide to start to do some work is whether whatever issue people see do fall within SSAC charter. So the question is – and we have been discussing a little bit universal acceptance issues and the question always comes back to does it really have – what kind of impact does whatever problem people point out have on the security and stability of the identifiers? And the question is whether usability falls there.

But this discussion we are coming back to over and over again, so it might be the case that we should look more into that. Thank you. And please introduce yourself.

[HIRO] Okay, my name is Hiro from ccTLD dot-jp and I'm a member of the [inaudible] project. Patrik, you mentioned about the IDN variance. Possible explosion of the number of variance which will be allocated as [inaudible] TLD. As I said, I'm involved in the LGR project, especially about IDN variance. How have you come to know about the possible [inaudible] variance? How have you found that, such issues [inaudible]? We think we understand those issues from our aspects, but I don't know whether our perception of such issue is sufficient or not. So we of course inform you if we think there are issues regarding security and stability.

I wonder, such communication cannot be formalized between you and community like us. But we need to communicate when we have [inaudible]. How do you think we can communicate about such issues?

PATRIK FALSTROM: Well, it is always possible for anyone to send a question to SSAC. That's how communication is happening. So the only organization – or sorry. We do have connection explicitly with a few groups. We have a liaison to the board. We have a liaison to ALAC. But apart from that, we do communicate – oh, yes, and then we also have ICANN staff from ICANN security team that is also participating in the work of SSAC.

But apart from those very limited connections that we do, anyone can ask us any kind of question which means that it is possible for either one of the panels or the integration panel to send us a question if that is something that they want to do and then we'll see how we respond.

Regarding the work with variance, SSAC have already made a couple of statements where we have pointed out, for example, how important it is to have one and only one set of variant rules for the root zone because we only have one of those.

But we don't, for example, say that all of those rules need to be there at the same point in time, but what is created is [forward] compatible if it is the case that that list is created [inaudible]. If it is the case that there is any other specifics in that case, a question [inaudible] asked us. This is, for example, what the discussion was about this morning. Is there anything that SSAC could look at regarding various issues? Anyone can bring up anything with us. Thank you.

DAN YORK: I would just comment on your point about the IPv4 squatting issue or people misusing it. I think that's only going to get much worse right now if people are not aware. ARIN is about to run out of IPv4 addresses in North America, probably like tomorrow.

PATRIK FALSTROM: Thank you very much. We agree on that and we also think the situation will become worse. We had a discussion in the meeting with ICANN board about not specifically the misuse of IP addresses, but if IPv4 addresses are moved around more than what it is now and misused more than what it is now, they will, from our perspective – we do believe and we had a discussion with ICANN board about this, there might be an increased interest from law enforcement to get authority data of who actually holds a certain IP address at each point in time.

This is something that of course is discussed in the RIRs, in their respective policy groups. But from our perspective, we think that ICANN is in a very special situation that ICANN do already have lots of experience working with law enforcement regarding WHOIS related issues.

And that knowledge that ICANN has is something that from our perspective, in one way or another, maybe can help the RIRs because we believe that the same kind of request from law enforcement in the interest of accuracy in WHOIS is something that might come up there as well.

At the moment, this of course – and this is also was the conclusion of the discussion of the board is so far the information has transferred by having individuals participate in both the ICANN process and the RIR process, but it also [inaudible] for both the board and also for us in SSAC that maybe it is the case that we have to do something, some information work together. But there was no conclusion. It was just a discussion. So, yes, we are looking very much into the end game of IPv4.

Anything else? Any SSAC member that would like to bring up something?

In that case, thank you very much for today. I give you back eleven minutes of your valuable time and see you in Dublin.

[END OF TRANSCRIPTION]