Transcription ICANN Beijing Meeting

Update from the Security and Stability Advisory Meeting

Sunday 7 April 2013 at 09:30 local time

Note: The following is the output of transcribing from an audio. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

On page: http://gnso.icann.org/en/calendar/#apr

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page

http://gnso.icann.org/calendar/

Jonathan Robinson: Can we start the recording? All right, thanks very much.

Welcome everyone to our second session of the day. Welcome to Patrick Falstrom, chair of the security and stability advisory committee and (Julie) from ICANN staff. Without further ado I'll hand over to Patrick for his update.

Patrick Falstrom: Thank you very much Jonathan. And thank you very much for inviting us. This is a recurring meeting that we are trying to have at every ICANN meeting, so of course I recognize a lot of familiar faces here -- not only in GNSO but also I see some SSAC members that have sneaked into the room.

So one thing I would like to start by saying is that we have members from SSAC 's side to over the years and during the meetings get more higher and higher number of SSAC members coming to the ICANN meetings. And looking at (Julie) I think we are about 20 this time approximately, yes.

Julie Hammer: (Unintelligible).

Patrick Falstrom: We're a little bit more than 20 out of 37 SSAC members are here on site in Beijing. So if it is the case that you have anything for example what I'm going

to discuss now that you would like to discuss with any of them please try to find them. Maybe we should have (unintelligible) hats or something to see who we are. Stickers, yes, we should have stickers, Mikey, yes.

So what we'll go through here today is first a brief overview of where we are. As normal, I'll do it as pretty quickly, because I think it's more important to discuss two of the reports that we issued recently. It's even the case that (SAC 58) was something that you probably haven't even had a chance to read but it's now available.

SSAC was initiated in 2001 and has been operating since 2002. We are an advisory committee of ICANN and as such provide guidance to the ICANN board and all the other SOs and ACs to staff and to the general community.

And our charter is to advise the ICANN community and board on matters related to the security and integrity of the internet's naming and address allocation systems. We are at the moment 38 members that are each appointed by the ICANN board for three year terms.

We have three committees or working groups that - of long term standing functions. We have the membership committee that is which is basically like a NomCom for SSAC that is handling all the requests that we get for memberships.

We have a group working on the DNS workshops that is at every ICANN meeting Wednesday between the approximate 9:00 and midday. We have participated in the working group of DSSA or is participating there. And there're also a couple other working groups where we have participated.

One thing I would like to point out is that yes you do see SSAC members participate in other working groups, but from our perspective it's really important to that the community separate between the cases where individuals participate in working groups and those individuals are also

SSAC, and when SSAC is participating that's a difference. And I know that you here in GNSO you do understand the difference between those kind of very important details.

What is SSAC statement is something that we make very few of them, but we ensure that they are as clear and as firm as possible. And while at the same time allow SSAC - individuals of SSAC with their skill set participate in as many discussions as possible.

We have work parties. And the task for the work party is to work on a specific problem statement or on a specific problem and try to see whether there is any issue. And the outcome of a work party can be either to respond a question from the board or from an SO or AC or something like that.

It could - the outcome of work party is often either a plain response letter. It could also be a report. And we will go through two of them today. Or the outcome could be that the work party come to the conclusion that what they were looking at is overtaken by events or we thought there was an issue here but by digging into it we see that no there is actually nothing here. So that we do have work party doesn't imply that there will be a report coming out. But these are issues that we are looking at at the moment.

We're looking at -- for example -- abuse metrics. We hear a lot of - we have heard during the years quite a lot of people saying there's a lot of abuse going abuse happening using domain names Whois and all different kinds of things. People say abuse, abuse, abuse.

We've been working together with law enforcement and meetings with law enforcement. And what we are trying to do is to come up with a better taxonomy. So two people that want to talk about abuse can easier to have a discussion on whether there is abuse or not by clarifying what we're actually talking about.

We're looking at the root (unintelligible) for the DN SSAC root. That is something that you've seen ICANN has a public commentary that is currently open regarding proposal from on how to do that. But we're also looking at the problem.

As I said we're meeting with law enforcement. We have through the last couple of years and also for 2013 applied for - sent in requests and participate in the internet governance forum in the fall - I'm sorry, at the end of the year in Bali this year.

The proposed workshop that we are going to work on this year has to do with general hygiene at scale which has to do with a discussion on what happens when too many, for example, open requests and resolvers access on the internet. That just one is close and they often request or resolve, but that doesn't really help. What do we do about it?

We're looking at success metrics for the new gTLD program. We are looking abuse of the DNS for DNS service attacks. And we might start things that look at the complexity and challenges in DNS given the various additions that people - and the various new usage that people see with DNS.

The last publication we done is SAC 58 and 57 that we have look shortly. We also did a few other reports that in the end of 2012 - during 2012 that you can see on the slide related to quantum blocking, dotless domains, senior character internationalized domain names. We also given some comments especially on the Whois review team final report. And the report on domain name registration data model.

Some of these things we already discussed at previous meetings. So if there's no questions I would like to open for quick questions. Otherwise we'll dive into the first of two reports that we'd like to go through today.

Man: (Unintelligible).

Woman: Yes, thanks Patrick. This is a quick question about SAC056, the discussion paper on quantum blocking. I thought it was excellent by the way. I'm just wondering if there's any ongoing work - or that's arising out of it that you might want to share or any opportunities for some, you know, other policies of input that might be a follow up to it.

Patrick Falstrom: In we in SSAC are not working on follow-ups on that content blocking. But I do know that other organizations have picked up what we were doing and they are doing continuation.

I know for example because I happen to personally participate in that work - I know that the council review for example is looking at an investigation regarding content blocking - I'm sorry cross bordering implications on various blocking technologies.

So I think more you'll see other organizations have started to look at our document and more in a more constructive way I would say look at the situation that yes if we recognize that we have distinct jurisdictions with each one having their own ability to come up with, for example, registration and what is lawful and non-lawful what kind of implications should that have and how does that play together with the fact that internet and communication is global. So I think the discussion is finally - and yes, I see Milton looking at me as well finally I see a little bit more constructive discussions here.

Woman: Thank you.

Patrick Falstrom: People still disagree as much as earlier but looking at more constructive discussions.

So with that, let me go into the reports. So SAC 57 is an advisory on internal name certificates. This is something that we have been working on since fall

of 2012. And it's the first time we do reports this way. And which means that the methodology we used is different.

The reason why we did it differently -- and I will show at the end of this what the timeline what kind of events happened -- it all started when we had an internal discussion inside SSAC and one SSAC member brought up this finding, and you could literally hear that everyone in SSAC took a deep breath and were so scared. So like it was so close to feeling that the sky is falling for new gTLDs.

So at the end of the day, we decided -- and I really mean that day -- that this is work is something that we need to handle under a normal disclosure policy that is very similar to the various (unintelligible) are using in the world. And we had a need for the first time to communicate with the affected parties with our recommendations long before we could issue our report.

This in turn forced us to understand how we are going to do this communication as we in SSAC are not operational. So we decided to work with the security team of ICANN and the good thing of course is that both SSAC individuals, many of the SSAC individuals if not all and the ICANN security team do have experience working in these kind of environments with the (unintelligible) and law enforcement.

So what we did was that we were working with the security team of ICANN. ICANN security team had to come up with the disclosure policy, and this is one of the reasons why that was pulled and published a month ago or something or two. The disclosure policy was then applied, and luckily enough -- that you actually will see at the end of this story -- people reacted the way according to our recommendation. So with that, let's go into the report.

So what we discovered was that there is for FSL or HDPS connections or web connections that have the you see the padlock being closed and similar for other protocols. What you do when you want a key or a certificate is that

you go to certificate authority and you tell the certificate authority that you would like to have a certificate for your domain name. And there's nothing weird with that. There are more than thousand - there are thousands of such certificate authorities in the world.

What we found - what we were looking at was the practice of certificate authorities to also give out certificates for domain names that did not exist in the domain name system. And this is something that enterprise has used internally. They use it like just because they need a certificate. You don't really need to tie it to the domain name system.

One thing that we checked was -- that you will see -- is how many of these were given out and we also discovered that quite a large number of these that already were given out were certificates for things that today are not domain names, but will be domain names when the new gTLDs are allocated.

So the real finding is that it was possible to request from a CA today a certificate for a domain name that will be available after the gTLDs are allocated.

And the reason - this is also the reason why we wanted to have like a disclosure policy here, because we found if we told this to the world a lot of people would of course immediately request for certificates for domain names and just go through the list of applications and request sort of certificates for those. And we thought wait a second we need to talk to the CAs and the browser vendors first.

So the reports says that we went through the - some of these investigations that exist and we found that at least 157 CAs in the world - this a lower bound. We have evidence that 157 CAs in the world give out internal name certificates without checking the new gTLD being applied for list of domain names.

The exact number of internal name certificates cannot be known, because the CAs don't disclose what certificates they're giving out first. Enterprises they - as I said use these internal name certificates for many different kinds of reasons. And as I said you can apply for a certificate, get it now, wait for the TLD to be allocated, set up your own web server on a wireless network or something, hijack the connection, present the certificate, and the people that are spoofed that get attacked by the middle man - in the middle attack get a padlock that is closed -- not very fun.

What we found during this investigation is that the CA Browser Forum -- which is an organization where the certificate authorities and browser vendors are -- they already knew about this. They knew about the ICANN new gTLD process. But they had decided to stop this practice by October 2016. And the vulnerability window SSAC's perspective is that the window for vulnerability would be at least three years, of course if not the gTLD process get delayed. But we don't believe that.

So we felt this was not good. So we asked the ICANN security team to immediately develop a plan, execute a risk mitigation plan. And now with the small print, that was the report. So what happened?

So we alerted the CA Browser Forum, ICANN, SSAC together with ICANN security team on 23 of January 2013. We explicitly briefed the CA browser forum at their annual meeting on 5 of February. They immediately created a ballot -- Ballot 96 -- on new gTLDs that was brought forward and was passed by the CA browser forum on February 20. So this was pretty quick action.

And the implication is that the CAs will stop issuing certificates that end in a applied for gTLD string within 30 days of ICANN signing the contract with the register operator, and CAs will revoke any existing certificates within 120 days of ICANN signing the contract with the records operator.

So this is what the CA Browser Forum - the decisions that they made. At this point in time, we decided that we - according to the disclosure policy that everything is now under control, and we could release the report which we did early March. That's it. Any questions?

Man: Thank you Patrick. Pardon my ignorance on this, but could you explain how the situation is different for new gTLDs? Why is it different for new gTLDs versus the TLD that in recent history have been put into the root like triple x or even going back to (unintelligible).

Patrick Falstrom: The answer is that there is no difference. We did not think about it at that time. So yes, it might happen for the other new TLDs. So you are absolutely correct. If that was your question, the answer is yes it could have happened.

And by the way let me say that this is one of the reasons why our ATF is working so hard on the technology called (DANE), which is putting the certificates in the DNS. And if the certificates are there and signed by DNS, that can be used instead of CA and the CA hierarchy to get the same kind of security.

So tie the certificates explicitly to the domain name would be helpful DNS. So this is why the last six months I've seen an increase in activity in the IETF in this area. So the engineering side I do believe that the way of handling TTIs with (ex 509) is this is just the first of many steps I think personally to that time is over when we could use that. Thank you.

Jonathan Robinson: Thanks, Patrick. This is an interesting area for obvious reasons. I just want to remind speakers to introduce themselves before they speak so it's caught on the transcript. Steve.

Steve Metalitz: Yes, Steve Metalitz with the Intellectual Property Constituency. Thank you for this presentation Patrick. I wanted - I'm trying to understand how if at all this issue fits in with the issue that was raised in the letter sent by PayPal I think

on March 15, which seems to be on a similar - is this the same issue or is this a similar issue? And if it's not the same issue, have you looked at that issue?

Patrick Falstrom: It's a similar issue. The - let me put it this way. The PayPal letter is a little bit more generic. So it's sort of covering this as well. The PayPal letter talks about sort of also the generic issue with namespace coalitions. So one of the things that we have had with the DNS is that we have had a hierarchal namespace with known top level domains. And that means that if you have other strengths separated by dots that looks like domain names, it hasn't been possible so far to know whether it is a domain name or this something that belongs to this other namespace.

But what is happening at the moment - and I think I haven't talked to Bill from PayPal since he sent the letter, so I don't really know really what's underlying that. But from now on everything that is a set of strings separated by dots can be a domain name, which means that we will probably see more name space coalitions. And yes, in SSAC fact we are looking at whether there are more things hiding than this.

And so to answer your question, I think what he writes in PayPal is a general portion that there might be other things in there. And yes we are taking it very seriously.

Jonathan Robinson: Jeff.

Jeff Neuman: Thanks Patrick for the update. Let me just ask I guess kind of a pointed question. Since the SSAC is responsible for advising the board, would the SSAC at any time use this - let me actually give a little more background.

Other people are using this SSAC report as yet another tool to argue that the (unintelligible) program should not go forward. You've seen some letters, filings and you've also seen rumors and discussions in the GAC and other places.

Let me just ask the pointed question. It's the SSAC going to use this report to advise the ICANN board not to move forward on the current timetable for the (unintelligible) process?

Patrick Falstrom: No.

Jeff Neuman: Thanks. I think that's a message that needs to go out there.

Patrick Falstrom: Absolutely, and I'm doing everything I can. I was chasing GAC members this morning.

Jeff Neuman: Great. We appreciate it. It is an issue. It's a big issue. It's one that seems like it's getting under control, and I think we need to stop those outside of the ICANN community. And even those inside the community that want to use it as a basis to delay. We need to make sure that they know the proper information.

Patrick Falstrom: The SSAC - given that the outcome of this report or sorry the outcome - the report is one thing and the outcome is another one, okay. So even though the report is - the report itself of course talks a lot about this is how bad it is. But that was - note that before we started to talk to CA Browser Forum.

Jeff Neuman: Right.

Patrick Falstrom: And if you look at this SSAC document itself it consists of two parts. One which is the report that we actually finished basically 1 of January. And then you have an Appendix A. what happened between January 1 when the report was done and when it was released, okay. And there you can see that for example the CA Browser Forum took action.

Jeff Neuman: Yes.

Patrick Falstrom: Okay, based on our report plus the actions we don't see any - we think this is resolved first of all. On the other hand we did point out that with implicitly just like we - just like I acknowledge the letter from PayPal and defining what we just saw could have happened with other TLDs as well. But there might be unknown namespace conflicts out there.

But on the other hand that is a risk that all of us know that each applicant that apply for a certain string there is some risk for that of course depending on what string you choose. So there's also - even though there is it might be the case - I'm not saying that I know of any because I don't. But if there is a risk with a specific string in that case like is it really ICANN on how much actually is the applicant that takes the risks because it's also business risk and whatever.

Jonathan Robinson: Thank you Patrick. Joy.

Joy Liddicoat: Joy Liddicoat NomCom stakeholder group. Patrick (unintelligible) presentation and thank you for it. Just a point of clarification on the actions taken by the CA by the forum. One is is the forum a forum of all certificate authorities, or is it more of an association of those who are like-minded and joined together? Appreciate it.

The second is it seems that the action taken by the CA forum was some kind of (sort of educating rather than) (unintelligible) obligatory in some ways. In other words should this statement that would basically stop issuing certificates. So is this the (unintelligible) that function, I guess is what I'm asking. Or is this something that sort of out of character that its (unintelligible) up to help us.

Patrick Falstrom: It's more like an association, so it's not a binding - it's not the case that all CAs must be members there. On the other hand, the whole idea with the certificate authority is for example that certificate authority's according to their agreement with the CA browser forum, a certificate authority should validate

in one way or another that if you request a certificate tied to a certain domain name, that you actually is the holder of that domain name.

And normally they do that by sending an email to well-known email address to an email address in that domain name. But any CA can make mistakes. They can intentionally or unintentionally give you the certificate anyways, which means that the CA browser forum have no way already today to actually sort of police that.

And we have had some issues where - as you know there's some well-known cases where CAs have made mistakes - technical mistakes of something else. And so it's the same thing here. To be a CA, you need to behave well. And that implies that you're following the rules. That's their control mechanism.

Jonathan Robinson: (Unintelligible) Thanks Patrick. Do you have some more slides to cover? We're a little short on time, so I just wanted to check if there was anything else.

Patrick Falstrom: I think we should just, because we're short on time we should just send this report to you, and we can discuss this sort of in the corridors when you find people and staff otherwise we will not be able to make it in time.

So I would like to thank you all and we'll be here as I said more than 20 of us are here this week. So you can just stop us at any time.

Jonathan Robinson: Thank you very much Patrick and (Julie). I mean you're certainly working a few of us up especially with that last issue which I know is on most people's minds. So thank you very much for your presentation.

You can stop the recording now.

END