DURBAN – GAC Meeting with SSAC
Tuesday, July 16, 2013 – 09:00 to 10:00
ICANN – Durban, South Africa

CHAIR DRYDEN: Good morning, everyone. Please take your seats.

So this morning the GAC will have an exchange with the Security and Stability Advisory Committee and they're going to present to us on what we think is the most important issue for us to be briefed on.

There are several areas of activity within the SSAC, but we want to make the best possible use of the short time we have available to us this morning to meet with the SSAC.

So without any further delay, I will hand over to Patrik Faltstrom, who is the chair of the Security and Stability Advisory Committee.

So over to you, Patrik.

PATRIK FALTSTROM: Thank you very much, Heather. And thanks to all the GAC members that have given us the opportunity to meet with you.

I'm the chair of the Security and Stability Advisory Committee of ICANN, and to the left of myself I have Jim Galvin, the vice chair.

SSAC was initiated in 2001 and began operation in 2002. We are an advisory committee, just like the Governmental Advisory Committee that you belong to.

Our charter includes that we should 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 currently 39 members, appointed by the ICANN board for three-year terms.

Just because of the limited amount of time we have and the fact that you already got some material from us, I would like to stop there and ask directly if there are any questions on the GAC itself and our operation.

So I don't see any question, and so with that I would ask to have the presentation about internal -- advisory on internal name certificates.

This is our document number, 57. And the way we are producing documents is we form working groups, or what we call work parties. And each -- And the work party is working on something that can result in a document.

When we have consensus in the work party, and later SSAC as a whole, on the document, the document is released.

It is possible for SSAC members to recuse themselves from the discussion on the document and to request an objection to be added to the documents. This has happened a few times, but normally, we in SSAC manage to reach consensus of documents.

This is one such document that we have consensus on.

This specific advisory identifies that a certificate authority that hands out certificates that are used for secure communication, specifically for

Web sites but also other protocols, if it is the case that that practice is widely exploited, that could pose a significant risk to the privacy and integrity of secure Internet communications. And this CA practice could impact the new gTLD program.

And in this report, we recommend ICANN to take immediate steps to mitigate these risks.

This report was finalized around beginning of January 2013.

Next slide, please.

So we took this report and handed over to ICANN, and following this SSAC advice, ICANN took immediate mitigation actions to reduce this risk. However, there are some residual risks that remains, and much more work needs to be done to address them.

Next slide, please.

Oops, okay. Go back.

So in short, what this report is about is that there has been a practice among certificate authorities to hand out certificates for domain names that does not exist in the DNS. And this report describes what happens if it is the case that certificates that are handed out for domain names that not yet are in the root zone later become delegated, as in the new gTLD process.

The technical explanation of what happens is that you have a certificate for one domain name that when the domain name itself later is delegated covers a service and secures connection to service to which -- for which the certificate was not issued.

There are many people from SSAC in the room here which are happy to discuss this with you.

The mitigation strategies that ICANN launched include communication and collaboration with the CA browser forum, which is the organization for certificate authorities and browser vendors to come up with policies on how to act and how to change the practices so that the risk is minimized.

There. Thank you.

Any questions on that?

CHAIR DRYDEN: Thank you very much, Patrik.

So I'll start off with a question but I see Italy is also asking for the floor.

But my question to you, because we're in the middle of -- well, near the end or at the end of the new gTLD program, how does this issue impact the current program or applications that have been made?

PATRIK FALTSTROM: What we identify in the report by doing searches on what certificate is -- certificates exist on the public Internet, we do see that certificates have been issued for domain names that now are applied for in the new gTLD system.

The further investigation of the implications is something we talk a little bit about in this report, but some of the mitigations, including the policies that CA browser's forum agreed to, which includes stop with

this practice and also to revoke the certificates for CAs, is, as we are saying in SSAC, is reducing the risk significantly. But there is still a risk that certificates exist for these existing -- for those domain names that are applied for.

CHAIR DRYDEN: Okay. Thank you, Patrik. Italy, please.

ITALY: My question was exactly the question of the Chair, so thanks for the answer.

CHAIR DRYDEN: Okay. U.K., please.

UNITED KINGDOM: Thanks very much, and thank you, Patrik, for alerting us to this issue. I mean, it seems quite a significant problem that's been hit upon here. But I'm not quite clear what the likely best course for resolving it is going to be. I didn't quite catch that, if you touched on it. So forgive me if I didn't follow clearly myself.

But is it a matter of some specific applications being put on hold while you research the solution to prevent any instability in the system? Is that the best course? And then what will be the likely frame, I guess is another question that certainly the applicants would want to know.

Thanks.

PATRIK FALTSTROM: From our perspective, from what we in SSAC are saying is revoking the certificates that exist there will work for the applications, for example, that actually validate those revocation lists, which is revocation as in invalidating already issued certificates. That's one of the mitigation methods.

The other one is, of course, to stop issuing these certificates, which is the other policy. So all of these things together minimizes the risk that these certificates are live and out on the Net.

Waiting or searching for these certificates will really not work because many of those certificates are unused internally in enterprises and not visible on the Internet. So when searching, you will always only see very few of them, or few of them, and no one really knows how many. You will still only see the ones that are exposed to the public Internet, sometimes by mistake and configuration errors by the local -- by the enterprises that do these configuration errors.

So this, from SSAC perspective, what we write about in the report is that this shows that the current system of trusting certificates do have issues. It's similar issue to, for example, you might have heard about the DigiNotar incident and others when certificate authorities themselves do have security breaches. And this is why lists of certificate authorities that are trusted, which is what the Internet uses at the moment, is a very instable mechanism to use for trust.

Distribution of trust as defined by the Internet nowadays is done via, for example, the Domain Name System with the help of DNSSEC, and then

used in more modern technology, DANE, where the information on what certificate is really in use for each domain name is stored in the DNS itself, and signed by DNSSEC.

So the real solution that we are pointing out in our report is to start to use DANE and DNSSEC, and what I would call inherit the trust from the DNSSEC hierarchy and DNSSEC and use that as information of what certificates you should trust instead of using lists of trusted parties that are updated very slowly, you get delay in the updates, and during the delay you might have vulnerabilities and attack factors.

CHAIR DRYDEN: Thank you for that response, Patrik.

Are there any other comments or questions on this presentation?

U.K.

UNITED KINGDOM: Thanks. Just a quick follow-up.

What is the scale of use by businesses with internal servers that creates this conflict? I mean, are we talking about hundreds of companies? Thousands?

I mean, what -- There's going to be a business impact, isn't there, of trying to correct this. That's my understanding from this.

PATRIK FALTSTROM: There are two different answers. First of all, regarding the actual wording, I must admit that just because we released the report in the January to March time frame, I'm sorry that I don't remember the numbers on the top of my head. So I would refer to the report so that I don't say something and the report says something else.

But the finding -- The reason why we issued the report is that we found that the usage is quite large; okay?

That said, the conclusions that we have is also that these mitigation methods is probably solving the problem as good as possible. So there is an inherent problem with the technology in use, which means that we cannot make it much better. There is a flaw there in that way of doing things, and that's why I'm saying waiting is not -- or delaying the introduction of TLDs or something doesn't really help.

Now, you may be, without thinking about it, asked a different question, slightly different question, and that is what happens if a company or enterprise is using, for any kind of use, a domain name that today doesn't exist in the Internet but later will be delegated?

Okay.

That is something that we have been looking at at SSAC, and it's also the case that we have a Board resolution and request for a study on name collision issues.

So you should read the internal name certificate report as one example of these name collision issues.

And the question on what happens when a domain name is delegated that is in use, for example, in a certain enterprise, yes, that will have some impact due to various technical reasons, like search path and other kind of things.

But ICANN has, on the request of a Board study and also an earlier SSAC report, SAC 45 that was issued fall of 2010, is looking into that namespace collision issue to see how -- how much that actually -- or what kind of risk there is based on that namespace collision issues.

CHAIR DRYDEN: Thank you.

So next I think it's Malaysia, yes, and then Netherlands.

MALAYSIA: Hi, thank you. Okay. I am from Malaysia.

I have a question. Maybe some of my question already answered, but I would like for you to explain a little bit about what is the impact to the end user of this problem with the certificate authority. That would be helpful.

Thank you.

PATRIK FALTSTROM: The impact of the end user for the certificate issues, the absolutely worst thing that can happen is that the end user do connect with, for example, the Web browser, to Web site. You see the padlock is locked, and you do believe that you have a trusted communication, but in

reality the connection is to not the site that you believe but to another Web site. That's the worst thing that can happen.

There are -- The reason why we, in SSAC, say that there are still some risks, but we still think that there is quite a lot of mitigations that there are multiple other attack mechanisms that might fool the end user that they do have a secure communication. So I would say that we have -- To answer your question, no, we have not evaluated that risk compared to others.

CHAIR DRYDEN: Thank you. Netherlands, please.

NETHERLANDS: Yes, and thank you, Patrik, for this presentation.

I have a question. What do you expect from the GAC? I have the impression that you have -- that the SSAC has been, let's say, really put the finger on this problem and has initiated some actions or so. And also, you said on the communication side that ICANN will intimate, let's say, further actions. What do you expect from the GAC?

PATRIK FALTSTROM: So I don't have any specific expectations from GAC, but I do have expectations from the ICANN community as a whole, where, of course, GAC is included.

The namespace collision issue is serious. And that is something that has been pointed out in many documents. If we look at what we have done

in SSAC, both SAC 45 from November 15, 2010, and SAC 57 from March 15, 2013, which is this namespace -- sorry, internal name certificates document, are talking about, and other documents.

What is happening at the moment, though, is that ICANN issued a study to investigate what the actual risks are with name collisions. That study is, as far as I understand, almost finished and handed over to ICANN. And we, just like other groups in ICANN, are awaiting to see the result of the report, the conclusions that are drawn on the basis of the report. And we are asked, SSAC, explicitly by the Board to comment on whatever conclusions are drawn, suggested changes in whatever documents.

And I personally expect that we will see some kind of public comment period, for example, on the findings and/or conclusions. So I just want everyone, including GAC, to keep their eyes open and comment on that if it is the case that GAC and others find that being necessary.

But we in SSAC are explicitly asked to say -- to keep our eyes on this and make sure that we believe that the study and the conclusions and everything is done in a sound way from a technical security and stability point of view, which is our charter.

CHAIR DRYDEN: Thank you.

Next I have Sri Lanka, please.

SRI LANKA: Thank you, Chair.

Good morning. I am Jayantha Fernando from Sri Lanka, a GAC rep. Firstly, I thank Patrik and your SSAC team for the excellent work you are all doing in this connection. I just have a short comment and a suggestion.

Although we are one of the first country codes to be DNSSEC signed and operate in that environment, we find many banks and organizations on the other domain systems. And in that context we also have a CA environment being built up.

So we have now a situation where they are looking out to greater cooperation. And is there some way your practice statements can feed to CAs operating in developing country environments? And maybe GAC can provide an environment or a platform through which that information can be disseminated to CAs either starting up operations or functioning in developing country environments. Just a comment, but what is your view on that?

Thank you.

PATRIK FALTSTROM: As I said earlier, we in SSAC do point out in our report on internal name certificates that we don't see any 100% solution on the certificate issue if we continue to use certificates the way we have been doing it so far with lists of CAs that are trusted.

What we say is one path forward is, instead, to use mechanisms like DANE, and that's where you have the technical connection between DNSSEC and certificates.

One path -- or moving forward, which I'm now speaking personally, because this is something that we have not talked about in SSAC as a whole, is that what is possible is for a domain name holder within your country to get a CA from your local CA in the country, but then take a fingerprint or a hash of that CA, store that with the help of DANE technology in the DNS, sign up for DNSSEC, and that way telling other people on the Internet that are connecting to that Web site, looking up the domain name, that's where, in DNSSEC and in DNS, the client 2, whoever has -- the customer of whoever has the Web site, will find in DNS and validate it with the help of DNSSEC that the right certificate has been used.

So the trust is coming from DNSSEC and the fact that a fingerprint is stored in the DNSSEC signed record and not because the CA is trusted. Because today I do see that CA is not only in developing countries but in many countries, including Sweden, sometimes have a problem to be able to get out in the market. Because today a CA must end up on one of those lists where you have trusted CAs, like inside browsers in operating systems. And that is sometimes a very hard job for a CA, because they want to concentrate on selling their certificates and have a sound and secure operation. And maybe that is -- that is what they want to concentrate on and not to fight to end up in all of those browsers and end up on these trusted lists. Thank you. So, yes, I do see a connection there that specifically can help start-ups and innovation in the CA and security environment.

CHAIR DRYDEN: Thank you for that. Are there any other questions or comments from the GAC on this issue? Iran, please.

IRAN: Thank you, Madam Chairman. And thanks for the presentations and clear answers given.

I have one simple question. How you could ensure that the domain function within the terms or within the terms and conditions which is stipulated in the certificates in a sense that is there any possibility of not complying with that? If the answer is yes, how you could monitor that and make it possible that terms and conditions are properly implemented and followed. Thank you.

PATRIK FALTSTROM: I can only answer from a DNS perspective. There are, as I said earlier, agreements within the CA browser forum on the best practices for CA authorities and CA certificate authorities. I don't know the policies and what kind of auditing they are using for agreements within the CA browser forum. So you need to talk to them about that. Regarding the DNS, the certificate itself includes the domain name that the certificate covers. Today that domain name in a certificate can include any domain name whatsoever, which means that the binding between the certificate and the owner of the certificate and the domain name is a validation that the certificate authority is doing. And that's where the policy stays. So the auditing is for the certificate authorities that they are following this policy.

This is why we're pointing at this new technology, DANE. Because what DANE is doing is allowing for the certificate owner to put a fingerprint, a check sum of the certificate in the DNS under a specific domain name and sign that with DNSSEC.

So when, for example, if I have done that as a certificate owner and you connect to my Web site, first of all, you use my domain name. You validate with DNSSEC that the DNS record you got back was correct. Then you look in that DNS record for the fingerprint of the certificate that I have put in DNS. You check the DNSSEC signature of that fingerprint so you know the fingerprint is correct. So now you know the domain name, and now you know what certificate it is. Then you check -- then you fetch the certificate.

Here's the tricky thing. Here's the key thing. You check the domain name inside the certificate and check that that domain name is the same as the domain name that you were looking up that you have validated with DNSSEC. And, if those two are the same, then you can know that the certificate is really issued for the domain name that you also tried to connect with the help of DNSSEC, which means that, with the help of DNSSEC, you got an extra ability as the end user to validate that the certificate authority were actually doing the right thing. And that's why it's really important. Because today a certificate authority can issue a domain name for any domain name that is out there. Of course, they don't, because there's an audit of them and self-control. But we engineers like extra technical measures to secure those things.

CHAIR DRYDEN: A follow-up from Iran?

IRAN: Yes, a follow-up. If it is not the same, then what you have to do? Or what is being done? Thank you.

PATRIK FALTSTROM: Today with DNSSEC, if it is the case that a DNSSEC response, a signed response does not validate, you as the client, will not get the response at all to your computer. So today, when you use a browser, you often get -- you probably have got this screen up. Oh, this is insecure. Do you want to continue? Yes/no? Everyone will click yes. Okay. In the new technologies, you will not even get that. So the end user is protected. But, in some cases, you will get the same kind of information to the end user or the application gets enough information to be able to inform the end user that they're moving into an insecure communication, which, of course, as we all know, sometimes you actually prefer to be able to communicate because the communication itself is really important as long as you know that it might be insecure.

CHAIR DRYDEN: Thank you for that follow-up question and response from Patrik. Okay. Are there any other questions that GAC colleagues might have?

PATRIK FALTSTROM: Are we done?

CHAIR DRYDEN: Yes. We do have the reports available to us that the SSAC has been working on both internal name certificates and name collisions. So that's a good way, I think, for the GAC to do additional reading on this.

And I know that, if there are further questions or things that the GAC would like to raise, that the SSAC will be responsive to that.

PATRIK FALTSTROM: I would like to, at this time, just like at other meetings, inform you that we have, I think, almost 20 SSAC members out of the 39 here on the floor here in Durban. And all of them are happy to talk with any of you. So you don't have to chase down me specifically. For some of these topics, they're actually matter experts in SSAC that know the details much better than myself. So don't hesitate trying to find any if you want to have clarification. Because that is what we are -- what I think we should use these face-to-face meetings for, the high bandwidth communication, take the reports, sit down with an SSAC member and go through and ask them so you really understand what the recommendations are. Yes. Oh, actually, good idea. Can the SSAC members in the room please stand up?

So this is what we look like.

CHAIR DRYDEN: A fine group of people. Okay.

So thank you for that. I see a question from Australia. Okay. Australia.

AUSTRALIA: Thank you, Chair. And thank you, Patrik. It's been a very interesting discussion. I'm just interested as we seem to have a couple minutes at the end and we didn't get to cover it yet. There's an SSAC report on dotless domains. And I keep hearing comments about dotless domains

here at the meeting. I have read the report, and the SSAC's position appears to be pretty clear. There's a strong recommendation against their use.

But I understand that, since the SSAC's report, there is continuing work and thought about this. I'm wondering if you can fill us in to where things are at with dotless domains.

PATRIK FALTSTROM: So the -- thank you for the question, Peter.

First of all, the applicant guidebook says that dotless domains, which is what we call it in SSAC, is something that is not allowed unless the applicant can demonstrate that their use is safe.

We in SSAC had a look at that and made an even stronger recommendation that the default absolutely must be that delegation -- that use of dotless domains should not happen.

During the public comment period that ICANN staff launched, based on our report, there were some responses from some vendors that even stronger said that if it is the case that dotless domains were in use, in that case for many, many, many end users, their local environment will break.

So there were vendors that, basically, admitted that their applications were drawing specific conclusions on dotless domains that implies, for example, that, when using a dotless domain, that domain name that the client uses will not even become a DNS query. Because dotless strings are interpreted by the applications as something else than a domain

name. For example, if you go to a browser and just type in one word without a dot, it will do a search. Okay? So that's the distinction.

So after that the board asked ICANN staff to issue a report on what the business or economic implications would be. And there had been some dialogue on that. What happened this spring was that that study -- a study was commissioned by ICANN staff on dotless domains that, if I understand correctly, is ready but not publicly available. So I don't know the result of that.

But, in parallel with that study being launched, the Internet architecture board wrote also a document based on the standards that we're using on the Internet for various protocols including electronic mail. And the Internet architecture board also very strongly advised against dotless domains. So the number of documents that very, very, very strongly recommends against dotless domains increases. But note that the applicant guidebook from the beginning is also advising against it. So all of this discussion is not about a requested change. It's more indication of -- that the applicant guidebook was correct.

CHAIR DRYDEN: Thank you for that. Argentina, you were next.

ARGENTINA: Thank you, Chair. Thank you, Patrik, for the presentation and congratulations for all the work you do. I have a question for the group. How are the members of the SSAC appointed? And I see the list, and I see only one member from Latin America. What we could do from our representatives in the GAC to increase that diversity in the group? And,

if it's a desire from the group to be more diverse -- and I see few women also -- what we could do to increase that. Thank you.

PATRIK FALTSTROM: So thank you for that question. We have one working group that we call the membership committee that my vice chair, Jim Galvin, is the chair of. And what we are doing is that we are receiving nominations so people can self-nominate or you can nominate other people. The people are interviewed. And what we do have -- specifically, what the membership committee have is a list of, I would say, like, skills or various issues that are handled through the MTU when you evaluate -- evaluation criteria -- let me put it that way -- that are in use. And, yes, both gender and geographical diversity is part of that criteria. But there are other things as well. For example, it's important for SSAC to have all together all the various -- all the skill sets that we need. So, for example, to be able to look at various reports. So, for example, there are people with very deep DNS expertise. We don't need more of those. But what we do need, which are, for example, the last couple people that have been appointed have been from law enforcement and also have been female.

So all -- but it's true that it is an internal process where -- that we have. And, regarding both geographical and gender diversity is something that I am myself, personally as chair, very disappointed on. So what can be done? By, like in many other cases, encouraging and reaching out to people to apply for membership in SSAC.

CHAIR DRYDEN: Thank you, Patrik. I have a few more requests to speak. And then I will need to, I think, close the session. So Singapore is next.

SINGAPORE: Thank you, Chair. Thanks, Patrik, for the work done by your group. I have a generic question. We know in the industry there are a few interest groups that monitors the safety and security of Internet. Notably, they are anti-phishing working group, APWG and PhishTank. Within this group there are list of those phishing sites. So we regularly check from this list whether any of our names are under a -- listed as a phishing site. So I would like to know is there any working relations between the SSAC and all these industry specialist groups? And, if you want to seek guidance, should we -- how do we approach? Should we come to SSAC or, you know, APWG?

PATRIK FALTSTROM: Thank you. That's a simple answer. No, we don't have a liaison or formal relationship with any other groups. That said, we have SSAC members which are also members of APWG. So we have a high volume of information sharing between SSAC and APWG and similar groups.

CHAIR DRYDEN: Thank you. Next Russia, and then I have U.K.

RUSSIA: Thank you, Chairman.

Patrik, I have a question regarding your advice, SSAC advice on dotless. Should it be mandated, or it's just soft advice because you know it can be applied only to new gTLDs because new gTLDs currently have haven't such limitations in real practice? Thank you.

PATRIK FALTSTROM: As everyone knows, just like you point out, the address records in the TLD were in the zone APEX, do exist on the Internet. And last time I checked, a few minutes ago, the Internet was still working. So, obviously, it's not killing the Internet. That said, there are, under very, very, very specific conditions that you can use an address record in a zone APEX without having secondary consequences, which means that I think -- and everyone knows that, specifically on the technical standpoint, no, there's no reason to completely ban it from the Internet. But there's -- but the risk is so extremely high that it must be encouraged to not use.

RUSSIA: Patrik, I want to clarify. It's more about game rules. Yes, it's clear from a technical point of view. And for me it's absolutely obvious that it's a problem. But it's about the rules. Because, if ICANN will put requirements for some registries and don't put specific requirement in action for other registries, it will be a problem.

PATRIK FALTSTROM: That is correct. But now we're moving into areas which SSAC -- which is not within SSAC's expertise which have to do with contractual

arrangement and how to handle contractual parties and others. And that's something that we in SSAC do not have any view on.

CHAIR DRYDEN: Thank you.

So, U.K., do you insist? We need to conclude this session. You had asked for the floor. Is that correct?

UNITED KINGDOM: Yes.

CHAIR DRYDEN: Can you be brief, please?

UNITED KINGDOM: And there's one aspect to this we hadn't touched on. And that is potential for criminal exploitation, which you referred to in conclusions. Do you want the GAC to give advice to the board to say "stop it"?

PATRIK FALTSTROM: What do you mean by "it"?

UNITED KINGDOM: The practice of dotless domains, which I think you expect new applicants possibly to want?

PATRIK FALTSTROM: I don't mind having GAC support, for example, the SSAC advice.

CHAIR DRYDEN: Thank you. Very concise answer. Okay. So thank you very much to the SSAC for coming to brief us. You know we always benefit enormously from these exchanges. And for the GAC we now have a 30-minute coffee break. Thank you.

**[ END OF AUDIO ]**