Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
29 March 2012 at 13:00 UTC

Note: The following is the output of transcribing from an audio recording of the DNS Security and Stability Analysis Working Group (DSSA WG) teleconference on 29 March 2012 at 13:00 UTC. . 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. The audio is also available at:
http://audio.icann.org/gnso/gnso-dssa-20120329-en.mp3
Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#mar

Attendees on the call:

At Large Members
. Cheryl Langdon-Orr (ALAC)

ccNSO Members
. Jacques Latour, .ca (CIRA)
. Jörg Schweiger, .de (co-chair)
. Rick Koeller, .ca (CIRA)

NRO Members
Carlos Martinez (LACNIC)

GNSO Members
. Mikey O'Connor - (CBUC) (co-chair)
. George Asare-Sakyi - (NCSG)
.Rosella Mattioli (NCSG)
. Rafik Dammak – (NCSG)
. Don Blumenthal – (RySG)

SSAC Members

Experts

ICANN Staff:
Glen de St Géry
Bart Boswinkel
Nathalie Peregrine

Apologies:
Scott Algeier
Jim Galvin (SSAC)
Mark Kosters (ARIN); (co-chair)
Olivier Crépin-Leblond (ALAC) (co-chair)
Andre Thompson (At-Large)
Katrina Sataki, .lv
Greg Aaron (RySG)
Luis Diego Espinoza,.cr

Coordinator: We're now recording.

Nathalie Peregrine: Thank you very much, (Ricardo). Good morning, good afternoon, good evening. This is the DSSA call on the 29th of March, 2012. On the call today we have Mikey O'Connor, Rafik Dammak, Cheryl Langdon-Orr, George Asare Sakyi, Jacques Latour, Rosella Mattioli, Jörg Schweiger, Don Blumenthal, and (Rick Keller).

From staff we have Glen de Saint Géry, Bart Boswinkel and myself, Nathalie Peregrine. We have apologies from Jim Galvin, Katrina Sataki, Mark Kosters, Olivier Crépin-LeBlond, Scott Algeier and Andre Thompson.

I would like to remind you all to please state your names before speaking for transcription purposes. Thank you very much and over to you, Mikey.

Mikey O'Connor: Thanks, Nathalie. As always making all the cool audio stuff happen leaves me in awe; it's great to have that going.

First up is our traditional moment where we pause and see if anybody needs to update their statements of interest. And I get to update mine today. Glen sent out the note. I am now a member - a shiny new card-carrying member of the ISP constituency in the GNSO changing over from the Business Constituency. Getting a little closer to my geek roots. So I'm not too terribly far away from where I was; just in a neighboring apartment.

Anybody else with a change to their statement of interest that we should know about?

All right. I think today what we're going to do - I did a bunch of stuff in the week that we didn't have a meeting that we're digesting in the ops group so I'm not going to dive into a bunch of the documents that I prepared because I want to give the leadership team a chance to sort of look at it and see if I'm totally off the track before I subject the rest of you to it.

So I thought what we would do today instead is sort of debrief on what we all learned at Costa Rica. And I've got a bunch of stuff that - I took some notes that are up on the screen that I sort of wanted to highlight for you and then to the extent that other people have ideas that flow out of that that I think would be a really useful thing to do this week. And then next week we'll dive into some of the stuff that will emerge from the ops group on Monday.

So what you see on the screen is the little mind map that I made for my - these are really notes to myself about DSSA stuff. And I think the one that really caught my attention in Costa Rica was this idea that we're building compound sentences. And I wanted to see if that caught other people's fancy as well.

Because I think it's a really - at least for me it was a - sort of ground breaking a-ha moment as a way to sort of plow through what is otherwise a very complicated methodology. And so I wanted to sort of highlight that idea.

And I thought that the name of the person who suggested it was Roy but I think it was really (Rick) who's on the call today. Have I got that wired up right now? (Rick), was that really your idea that...

(Rick Keller): Yeah.

Mikey O'Connor: Yeah, okay. Well I'm now probably going to call you Roy a few times before I get that name rewired in my brain and I apologize for that.

(Rick Keller): No problem.

Mikey O'Connor: And the question that came to me out of that as I thought about it was sort of when and how those sentences get built because it seems to me that one way to do this would be to - I built a little tool to do that which again I need to let the leadership team digest a bit before I throw it at you all.

But presuming that we come up with some sort of mechanism to build these scenarios one approach that I thought might be interesting would be to throw the tool out to all of us and let all of us come up with one or two compound sentence risk scenarios that are really interesting to us as individuals.

And draw those back together in a big pile and see if there are any patterns or trends in those compound sentences that we each as individuals create. And use that as a way to guide us to creating what I think would be a handful of risk scenarios that would go in our report as early candidates for deep review.

But I've never done this before. And so I wanted to sort of throw that back to Rick and Jacques and others who've done this sort of thing to see if that's the way those things are used or whether there's another approach to that. So I'm sort of putting you right on the spot on your first call, Rick. But that's just part of the deal with being in the DSSA.

(Rick Keller): Yeah, that's fine, Mike. So it's (Rick Keller) speaking. So, yeah, that makes sense. You know, the approach I took here at (Sero) was just to have people identify risks and then we started to structure them as compound sentences, you know, using a consistent kind of format.

So I think you're on the right track.

Mikey O'Connor: So once you structured them what did you do with them? Did you then do an analysis around each sentence basically?

(Rick Keller): Yeah, I mean, you know, in a single organization what I did was I went to all of our business units or all of the relevant sort of stakeholders in the company and I asked everybody to identify their top three which built out a register of dominoes, some duplication.

And, you know, we - so first of all I built the methodology and then started to identify risks and then started to evaluate the risks.

Mikey O'Connor: Yeah, I think that's - I'm glad to hear that because I think the other way to do it would be to go through each of the components of the compound sentence first and - essentially that's what we were doing. And I think that got us pretty bogged down. We spent a long time looking at vulnerabilities and then we took a long time looking at threat events.

And I'm thinking that it may be easier for us if we start by assembling the compound sentences because then we will be able to pretty quickly run into things that need to be refined in the methodology and fix those as we go. So I'm encouraged to hear that.

Does anybody else have any reactions to this? There's a tool on the way but again I don't want to flash that in front of you until the leadership group has had a chance to take the rough edges off of it. But in terms of an approach I'm quite intrigued with this. And just want to take a moment to see if other people have either had experience with something like that or have any reactions to this idea.

One of the things I think then that starts to emerge is that we have a report that we aim for at Prague - an initial draft report that goes into a fairly extensive description of the methodology and the actual risk framework and

then contains a handful of these risk scenarios that we've basically spent the next - we have effectively about eight weeks between now and Prague to do stuff.

And my thought is that we would spend a lot of the time working on these compound sentences and that that would be another major piece of the report. Okay well I won't belabor this. And stand by for treats next week because I do have a little tool that I built to do some of this stuff.

Jacques Latour: It's Jacques here.

Mikey O'Connor: Go ahead, Jacques.

Jacques Latour: So we're going to pull (unintelligible) on the three threat events right around the zone?

Mikey O'Connor: Yeah, absolutely. I didn't - the one thing that I did on the threat events is - and you can see it. One of the conversations in - oops - in Costa Rica was that there are really two threat events.

Jacques Latour: Okay so I still think there's three. Like (zone) does not resolve, is incorrect and security is compromised. I think those are three distinct threat events.

Mikey O'Connor: Okay.

Jacques Latour: I didn't necessarily agree with (Ross).

Mikey O'Connor: Okay.

((Crosstalk))

Jacques Latour: Jörg, what's your take on that?

Mikey O'Connor: Nice job putting Jörg on...

((Crosstalk))

Jörg Schweiger: Fiddling around as always. Hi folks. Yeah, Jörg, for the transcript. I think that the intervention was kind of reasonable. And I can live with it. And I think we already gave a possibility of how this could be phrased. And I think we ended up with something like availability of the zone and integrity. And that would be just fine for me for sure as it was...

((Crosstalk))

Jörg Schweiger: ...as a reaction to (Russ)'s input. I can do it as fine as long as we do summarize the points we had before under those two so security is, yeah, is a concern. But I might neatly sum it under the term integrity.

Mikey O'Connor: I don't have real strong feelings either, Jacques. But it's not to say that the security item has been lost. The sense that I got from (Russ) was that he was really more focused on the structure rather than the content that, you know, we certainly want to have a way to talk about things like DNS SEC. And that - at least what I took away from this at the meeting in Costa Rica was that we would just put that underneath the integrity one.

What are the big three? It's availability, integrity and blank.

Jacques Latour: Security.

Mikey O'Connor: No, the example that comes to mind is the revealing of private information. But that...

Jacques Latour: Privacy.

Mikey O'Connor: Yeah, in the security lingo there are three words that go together. And one of the things that fell out of the...

Rosella Mattioli: Confidentiality.

Mikey O'Connor: Pardon me?

Rosella Mattioli: Confidentiality...

((Crosstalk))

Mikey O'Connor: Confidentiality that's the one. I knew that there was. And one of the things that I think we'll want to talk about is whether there is a confidentiality leg to our threat events or whether because of the nature of the zone there is no confidential information in it and thus the standard confidentiality leg of threat events drops out. That's a puzzle for - that I've already built into the report outline.

But I think in terms of the security side it's fine with me to put it inside the integrity piece as long as we don't lose it. And I don't think anybody wants to lose that.

Jaques Latour: So, Mike, the - I guess I'm okay with that but I just want to raise one point is if - for some reason let's say the private (keys) for a zone in DNS SEC are compromised the zone is still - the integrity of the zone is still valid; that means it can - it resolves. It's valid. The signatures are accurate, everything is good except the threat is people can generate new signatures or steal your information or whatever. So I - it's...

Mikey O'Connor: Oh and maybe that's the confidentiality angle. You know...

Jaques Latour: So that's - I'm okay either way but I want to make sure that that might come back...

Mikey O'Connor: Yeah, no I think that's a good. Just type that into my little notes so that we don't lose that. Because I don't think the intent was to lose that topic; it was really more just an organizing thing. But I think your points are quite valid, Jacques. So we'll leave that in the pile to continue to discuss.

Okay let's see. Now another thing that I've done in the drafts that are coming - I hate to tease you like this but I really do want to leave another meeting for the leadership group to take a look at this stuff - is some of the impacts that we described were a little sketchy. And so I went back into the methodology. The methodology is quite deep in terms of examples. So I've pulled a bunch of examples forward that you'll see in the draft. So that was just a note to myself.

But one of the other things that I ran into is that there is another methodology that's at least as big as the one that we're using maybe bigger that focuses - and it's a related methodology, it's another one in the series of documents that the methods that we're using right now came from. And this other one focuses entirely on vulnerabilities. And it's simply gigantic.

And as I looked at that I realized that this might be another one that we want to add to our list of methodologies that we are using as the basis of our report. And I'll - when we get to it I'll give you a tour of all of that.

But if I were in the shoes of a person charged with actually, you know, actually responsible for security the vulnerabilities one was actually quite a bit more useful to me because it gave examples of all sorts of things that I could do to mitigate risk.

And so, you know, I think that's another topic that we're going to want to get into is - and let me segue into sort of another big thing that came out of Costa Rica for me and that is sort of the role of the DSSA both now and forever into

the future. The DSSA is chartered as a project. It's got a beginning, a middle and an end (unintelligible).

But the first draft of the SSRT report is now out. And one of the interesting things in that report - which by the way I commend to all of us to read because it's got a lot of really interesting ideas and points some of which bear on our work. One of the things emerges in that report is almost a presumption that the DSSA is an ongoing group rather than a project.

And that's something that we as a working group are going to have to navigate because we're not chartered to be an ongoing group. But at the same time there are a bunch of useful things that could be done on an ongoing basis that a group like us might be able to do.

And so we've got sort of another big question - bigger even than the analysis questions is the sort of relationship questions between us consumers and providers of the DNS at the very top level that we have to noodle through I think.

And so in parallel with creating the compound sentences and refining our methodology I think we've also got, you know, this sort of meta issue which is how does this kind of work get done by whom in the future.

Oh and Cheryl has got a point in the chat that's absolutely right which is the vulnerability stuff can - is great - absolutely amazingly great for the go-deep phase which will come after Prague.

And I think that one of the things that we'll discover when we go deep is that there's no bottom to the well that when we say go deep we're still not going to be able to go all the way to the bottom because there really is no bottom. And...

Cheryl Langdon-Orr: Mikey, I'd be more concerned if we could.

Mikey O'Connor: Yeah. Well believe me I don't think there's any bottom, you know, especially given the issues that emerged from this other methodology. It's overwhelming. And, you know, there are some really interesting puzzles in here one of which is the authority, accountability, responsibility puzzle.

Because especially in the case of the ccTLDs, you know, ICANN really has no authority whatsoever in terms of...

Cheryl Langdon-Orr: That's right.

Mikey O'Connor: ...any kind of action on the part of the ccTLDs. At the same time ICANN is a great place to build tools and models and share best practices...

Cheryl Langdon-Orr: Best practices...

Mikey O'Connor: ...and stuff like that.

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: And there's this sort of interesting place where, you know, I know that in earlier times people tried to paint a fairly authoritative role for ICANN in this area and it met with a lot of resistance from the community and I think correctly.

But I think that if we can step back a bit from that and think about positive contributions that the community could make without being an authoritative or authoritarian force that, you know, we could really move the needle a lot in terms of security.

So we have a lot to talk about between now and Prague. And I'm a little intimidated by eight weeks quite frankly because effectively, you know, there

are report deadlines and stuff like that that mean that we really need to be done - two months. And that's going to be a pretty brisk pace.

And so as I looked at the calendar when I was sitting on my beautiful porch - veranda in Costa Rica I decided that the thing to do was to write a first draft of the whole report as a very rough outline and then let us edit it and improve it for the eight weeks rather than trying to create it section by section.

You know, I'm treating this document sort of like a hologram where if you cut a hologram into a whole bunch of little pieces and look at it you can still see the whole image it's just not very clear.

And then, you know, as the - as you go towards a bigger and bigger version of the hologram the shape of the thing doesn't change a whole lot but the clarity and quality of the image gets better. That what we'll do is clarify that image for the next eight weeks and then present it in whatever state it's in with a big disclaimer that says, you know, this isn't done and it may never be done but this is where we are right now.

And so I went ahead and created that first draft. And again I don't want to get ahead of my co-chairs so I want to save that for next week. But that's sort of the approach that has emerged for me. And in that is a discussion of this future, you know, the future of DSSA or its sequel.

Because in the SSRT report they refer to us in a different way than we really are. And I thought that I had made it pretty clear to Alejandro and Jeff Brueggeman and some of the others in there that we're really a beginning/middle/end kind of thing. But that didn't get through. And so we've got a bit of a puzzle there that we need to work through.

Anything else come out of Costa Rica for the rest of you? I've sort of done another one of the Mikey talking all the time things and I apologize for that.

But I did a lot of work on this stuff between the meeting in Costa Rica and now and I wanted to sort of share that in a general way with you.

But for those of you who were at the meeting and participated in some of the other meetings do you have any other observations that we should carry away from Costa Rica to fold into our thinking and our reports?

Jaques Latour: Jacques here. No.

((Crosstalk))

Mikey O'Connor: Go ahead.

Jaques Latour: Not much.

Mikey O'Connor: Not much, eh? Well I mostly want to check one last time on the go fast then go deep because that was the big conclusion that came out of Costa Rica. And if I don't hear any last thoughts on that I think that's - we'll put that issue to bed to see what's underneath some of these.

No I don't - I really don't want to go into any of the other stuff today because I really want to give my co-chairs a chance to look at it. So maybe what we'll do is wrap up just a little bit early today and pick it up again in a week unless there's any other business at all that people want to bring up? Because I otherwise find myself in the awkward position of talking about a document that I have but I don't want to share. And so as a result I...

((Crosstalk))

Mikey O'Connor: Yeah, I think it's easier just to wait. And so I don't know, with that anything else? We'll let people come back from the IETF and carry on in a week with the first look at the murky hologram. With that...

Cheryl Langdon-Orr: Sounds like a plan, Mikey.

Mikey O'Connor: ...I think we'll wrap it up.

Cheryl Langdon-Orr: Sounds like a plan.

Mikey O'Connor: Okay dokey. Well we'll see you in a week. Sorry about the short meeting but there you go. Nathalie, I think we can cut off the recording and call it quits.

Nathalie Peregrine: All right thank you. (Ricardo), could you please stop the recordings? Thank you very much.

END