Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
06 October 2011 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 06 October 2011 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-20111006-en.mp3
On page: http://gnso.icann.org/calendar/#oct (transcripts and recordings are found on the calendar page)

Attendees on the call:

At Large Members

●Olivier Crépin-Leblond
●Andre Thompson
●Cheryl Langdon-Orr (ALAC)

ccNSO Members

• Takayasu Matsuura, .jp
• Jaques Latour, .ca
• Joerg Schweiger.de (co chair)

NRO Members

• Mark Kosters (co chair) – on adobe connect

GNSO Members

• Mikey O'Connor – (CBUC) (co-chair)
• Rossella Mattioli – (NCSG) – on adobe connect
• Don Blumenthal – (RySG)
•Greg Aaron – (RySG) – on adobe connect
•Rafik Dammak, GNSO

SSAC

• Mark Kosters (SSAC) – on adobe connect
• Jim Galvin (SSAC) – on adobe connect

ICANN Staff:

Julie Hedlund
Patrick Jones
Nathalie Peregrine

Apologies:

Nishal Goburdhan (NRO)
Scott McCormick (IPC)
Bart Boswinkel
Katrina Sataki, .lv
Edmon Chung (ALAC)
Wim Degezelle, CENTR
Keith Drazek – (RySG)
Luis Diego Espinoza,.cr
Rick Wilhelm, Network Solutions
John Levine
Otmar Lendl, .at
Ondrej Filip, .cz
Arturo Servin (LACNIC)
Carlos Martinez (LACNIC)
Sean Copeland, .vi
Patrick Vande Walle – At large
Chris Wright, .au
George Asare-Sakyi – (NCSG)
Adam Palmer – (CBUC)
Andrew de la Haye (NRO Member) - for the next 4 weeks
Mohamed El Bashir (At-Large)
David Conrad (SSAC)

Coordinator: Thank you. The recordings have started. Please go ahead.

(Natalie): Thank you very much (Sam). Good morning good afternoon good evening. This is the DSSA call on the 6th of October of 2011.

On the line today we have Cheryl Langdon-Orr, Rafik Dammak, Andre Thompson, Mike O'Connor, Olivier Crépin-Leblond, (Jack Griffin), (Dakar Su Matzul), Jorg Schweiger, and Jacques Latour.

From staff we have Patrick Jones and Julie Hedlund. On Adobe we have Rosella Mattioli and Jim Galvin.

We have apologies from Sean Copeland, (Linda Gazela), (Katerina Zataki), Andres Phillip, Scott McCormick and Bart Boswinkel.

I'd ask you to please state your name before speaking for transcription purposes. Thank you very much Mike. Go ahead.

Mikey O'Connor: Thanks (Natalie) and just for the attendance record I think Greg Aaron and has either just joined the call or will be coming in. He's come into Adobe so we can add him to the list.

Welcome everybody. Our agenda is short and sweet but important nonetheless. Mostly we're going to focus on continuing the vulnerability scope discussion.

And then we've got a slide deck that we want to run by you that the co-chairs will be using in Dakar for the various status update meetings. So we'll take some time towards the end of the call to do that.

And Greg will only be on Adobe for the moment but he's at least with this. Thanks for that Greg.

So with that we'll stop for a moment and just check and see if anybody needs to tell us of about an update to the statement of interest and we'll go ahead.

Okay on your screen is the Vulnerabilities Mine Map. And I'm pretty sure that we'll be able to get through the rest of this today.

We really only have the three topics -- DNSSEC vulnerability of DNS software and bad players to get through in terms of our scope discussion.

And starting off with the first one I'm just having a kind of elderly moment. I don't know why that one - why we skipped that one last week. So if anybody can remind me that would be good.

But we at least need to decide what to do with DNSSEC. I'm not sure that I would call DNSSEC a vulnerability per se. Perhaps the lack of DNSSEC could lead to vulnerabilities.

Clearly if we decide that DNSSEC is an appropriate thing to talk about it would seem to me to be in scope since the top level and the root seem to be were the DNSSEC action is happening right now.

Oh, Mark Koster just joined us too so any thoughts on DNSSEC what we want to do with this? Potential yes, and in fact let me open this up.

Jim Galvin just topped - typed something into the chat saying oh, that's a little ugly. Let’s see how bad this is.

Here's what I captured. Can I fit it all - yes I considered on the screen.

Here's what I captured about DNSSEC. And Jim's comment is a potential DNSSEC vulnerability is your key management. If you don't do it right you go dark.

And Greg agrees yes the root assigned as well. (Jacque) is suggesting maybe this is an operational issue. Mark Kosters is saying yes pretty operational.

Jim Galvin isn't convinced completely. Says many management issues do this. Jim you may need to clarify that one a little bit for me.

This is an interesting call. I am the reader of the call I have everybody doing all the work in Adobe. I love this.

Agreeing that this is an operational issue so in scope and put it in the operational issues pile that seems to be where things are headed.

If you disagree this would be a good time to steer me in the right direction otherwise I'll put it in scope and take an action item to move it into the operational issues, going once, going twice.

Okay let me do that real quick. Just fix my little thing here.

There, good deal. One down two to go.

The next ones that showed up in vulnerabilities I think this came from originally from the meeting in Singapore in our group discussion there.

And then over the course of my rummaging I throw a whole bunch of topics into this, some of which may be in scope, some of which may be out.

And I can expand some of these just to give you a sense of what I was finding because I think it's a little bit whoa, that one gets a little bit. Oh there's DNSSEC again.

I think maybe what we'll do is we'll put that one up DNSSEC pile because we've got a whole pile. Come on little computer you can do this. Come on. There we go. Short pause while I rearrange my documents.

Whoa, there's a whole bunch of wildcard stuff. I guess it's too much to show on screen.

Anyway that's sort of the topic. And a question of the day is is this in scope and then if so I can find a home for it.

I'm less concerned about where it goes. Is there anybody I guess - one way to frame this is to say is there anybody who thinks this is out of scope? It certainly seems like there are a lot of things to talk about in this topic.

Oh Cheryl is typing in scope. Cheryl is saying in scope. Anybody think this is out of scope? That's what I would lobby for now otherwise I think we'll just go with the flow.

This one came a very early in our conversation and there's certainly lots of material under. Okay I'm going to put that in the scope and carry-on.

All right last one and again this is a first pass. I -you know, we had a conversation about some of this on the co-chair's call on Monday. And I should reemphasize that all of these are sort of a first time through conversation.

I think we may get some course corrections over the next few weeks especially in Dakar that we may want to fold into some of this. But we are on the home stretch here.

In vulnerabilities I'm just going to - we have a topic in vulnerabilities that we consider in scope called governmental interventions.

In there the subtopics are things like regulatory imposed shutdown, government seizure of regulatory registry operator, government takeovers, coups, political events, et cetera, state-sponsored and so on.

And I think that this topic, the bad players topic came up in Singapore. And with your permission I think I would tend to fold this one into the already existing area that we have in vulnerabilities.

But we could also have a separate - well first question I guess is whether this is in scope or not. And if it is we could sort out where we think we want to put it.

Again I think I'll call for anybody thinking this is out of scope. And I think clearly in terms of threats these are the kinds of sorts of threats that lead to the attacks.

So I'm getting some comments in the chat. Patrick, Cheryl and (Rosella) I think is in. So we'll do that. We'll put it in.

Let me copy and paste it into the other one while I'm thinking about it. All right so ta da, we've gotten through the first pass of the scope discussion. And we should take a moment and shout hooray.

There is some more stuff that I have stopped summarizing and I'm going to return to that. So I may come back to you on a subsequent call with a couple more additions to one of these lists because people forwarded a couple of ideas to me and I just haven't had time to summarize them.

But I think we've certainly covered the waterfront and thank you all for that.

So with that let's move on to the Dakar slide and let me show you what current draft from the co-chairs looks like and then see what you think.

I sent it out to the list and hopefully you all got it. It was a pretty big file. And so rather than enclosing it as part of the email for those of you who are on slow email connections I did a link to it.

So just step you through it really quickly. The purpose of these slides is primarily for the five co-chairs to go update their respective communities, sort of where we're at. But the thought is that we'll spend five or ten minutes walking through these slides and then take some time at the end to take some input.

We are also invited to join the SSR Accountability Review Team at 8:00 in the morning on Thursday. And we'll use these slides in that conversation just to kick that off as well.

So anyway just to give you a bit of an update on what these are about. So I repeat our sort of payday charter slide and then sort of give an update on where we're at.

This is a kind of informal guesstimate on my part. I think what we've just completed is about 70% of the identified threats work.

What we need to do yet is go through that again, make sure that it's really right, touch on ones that we didn't decide and then get the consensus on - well before we get the consensus one of the big steps in the work plan is to go out to the community and ask the community how are we doing on this, are we on the right track?

And actually that's the main point of this slide deck you'll see in a minute that a summary of our scope discussion is in here. And I think that's really going to be the focus of the conversation in Dakar.

So, you know, I think we're doing fine but we're not completely done with this first phase and so this is just a kind of project manager thing describing all that.

And then this is the Jorg Schweiger memorial show off how much work we've done slide.

We had - when you look at the results of our work it's very easy to come to the conclusion that we haven't done very much.

But those of you who have been on all these calls and dragged, you know, been dragged through all these conversations know that we've done a lot of work and it’s time to acknowledge that.

So I had fun making this slide and that's the reason this deck is so big is because these PDFs over on the left are pretty big.

For the transcript, Cheryl loves the George Bernard Shaw reference that said - the quote that says I'm sorry this letter is so long. I didn't have time to make it shorter.

Really what you all have been doing is making a really long document a whole lot shorter and a whole lot easier to comprehend. So it's worth taking a moment with our respective ACs and SOs and acknowledging that.

One of the things that we have done is refined our scope a lot both in all those individual statements that we've been working on but also just refining our understanding, our shared understanding of scope.

And so there's a slide on here that takes a piece out of the charter but then also takes a piece out of Greg's email that we talked about and so just a moment to highlight that.

Oh Jorg says that that quote is (Shiller Taga). I don't know, maybe it is. I was doing my Internet search thing and it popped up under George Bernard Shaw.

Just goes to show you should trust everything you read on the Internet I guess. Sorry about that Jorg, that could well be right.

So anyway then here's the summary. This is a couple of weeks old. So what I will do is I will go through and update these.

That's why it says draft all over. And it's really going to stay draft to Dakar. Because what we really want to do is show this to all of the community folks and get their reaction to our choices.

And I think that Patrick's got a reaction to one. And Patrick if it's okay with you let me step through all three and then we can circle back to this one.

We had a bit of a discussion about the business failure and the rationale for taking it out of scope. And so you may want to at least highlight this one.

And if we can agree we'll do something with it. If we can't we'll just move business failure up into the out of - the under discussion pile and get it fixed because there are a few things in here that are still under discussion as you can see.

So this is just a quick look at the threats direct attacks and then the indirect attacks one. And we have poor old email sort of hanging out there alone on this one.

We may want to when we get done we may want to move it into some other section. Patrick go ahead.

Patrick Jones: Yes Mikey can you go okay back up to threats on the underlying infrastructure slide?

Mikey O'Connor: Yes.

Patrick Jones: Okay good. So I made this point earlier with a small group. But I am not sure about the putting - well the rational statement for business failure.

It may well be out of scope but I think it seems like a rather strong statement to make at this stage because one, we don't have a lot of data, real world data on the failure of a registry so we don't know what either a smaller or a registry other than Commonnet may have on the infrastructure.

And another is it's just yes I'm not sure that that's the right rationale. So I don't know what others think about this. Maybe some registry operators the participate in the call have a view. But I'm wary of having a rational that strong for business failure.

Mikey O'Connor: Trying to get the actual PowerPoint slide up on the screen so that I can edit it. Okay what do people think about that, any thoughts on that particular topic? Oh good it's on the screen.

Jorg, Jim Galvin, Mark Koster's, Jorg says a business failure on a root level would certainly have an impact.

Mark says makes sense - Mark Koster says make sense to me to take it out of the rational part.

I just love this I get to be the reader. Multiple attendees are typing so we'll have a bit of a chat on the - thank you Mark. Mark says I'm doing a great job as a reader.

Anyway I think the question that I'd like to focus on is whether - what we're doing with this. Are we going to leave it out of scope? Are we going to move it back into still under discussion?

Either is fine with me. I think that if there's a problem with the rationale we can fix the rationale right now.

If there is a problem with in or out of scope then we should probably pull it back up under - well we can work on it today but at a minimum we should pull it into under discussion rather than leaving it out of scope.

Let's see Patrick says it could stay out of scope I think. We don't really have enough information to make that rational so strong. Let me capture that point.

Meanwhile lots of people have typed. Jim Galvin agrees that business failure at the root would be an issue. Cheryl agrees with Jim.

Jim thinks I think we should leave it otherwise as an open question or perhaps we'll get some advice during the public presentation.

Jorg is a good suggestion. Put it out for comment. What was Jorg's? Oh yes take it out to the community.

So that would be one way to do that is to move it up into under discussion and highlight it for discussion.

That's sort of where we're headed at the moment. Cheryl's agreeing. Okay let's do that. I'll move this one in there, change it to regular type.

Come on dear, you can do this. Good. All right I'm going to have to fix a lot of this stuff posthaste but I've got the idea.

Put it up there now. Okay anything else on the slide deck? Let's see how I'm going to show you things now that I'm on the PowerPoint thing?

I think I'm going to go back to the deck and then I'm going to give you - you can each have control of the deck yourselves and sort of use it to scroll up and down to check things.

So you can now individually move around in the document and just check and see (unintelligible) anything else on the - on this deck? Close enough for Dakar?

Jim and (Jacque) are typing. I may be missing. I did I missed a bunch of stuff. Patrick agrees with Jim on the put it out for comment.

Yes I agree Jim maybe we take the rationale off. Yes okay I get that. I just I missed that comment. Let me take that out of there. It's easy.

Oh now it's you can't see this because I switched back to the PDF version of the document. But the rationale is now and business failure is just under discussion.

So the ones that are under discussion right now are depletion of the IPZ4 address pool and underlying infrastructure.

IDF attacks and malicious or unintentional alteration of DNS configuration information in direct attacks.

Oh what in the heck is - oh yes okay. Again I lost myself in my own document here.

Okay so it sounds like this deck is okay with that change. I'm going to give you your last chance to say no thanks.

But the only change that we'll make to the document that's on the screen in front of you is that in the first slide of in or out of scope stuff we'll move business failure back under discussion with no rationale and take the rationale out of there.

Okay wow, I guess at this point what we could do - I hate to miss the opportunity to keep moving forward.

So if it's all right with you all since we have another half hour on this call I'm out of agenda items and my inclination would be to go back to discussing some of these under discussion topics because some of them we just didn't have time to get through properly.

So unless oh Greg is saying near the end of the call maybe we could talk about Dakar? Why don't we do that now Greg and then we can circle back to the ones that have that we didn't get to.

Oh questions of logistics and so on. Let's do the who will be there question. If you are going to be in Dakar why don't you go ahead and use the same - up in the center of this top of the Adobe screen there's a little raised hand thing and next to it is a agree.

Well yes, go ahead and raise your hand if you're going to be in Dakar or agree -- just some indication.

And if you're not going to be in Dakar don't indicate anything. So I see quite a number of people are going to be there. Way to go.

I'm not. Julie is not, Mark Koster's is not, I am not. Oh that's a good idea, use the X if you're not. I can use that too.

The X okay so (Natalie) here's so little action item for you. Can you write down the list of who says they're going to be there or not?

((Crosstalk))

Mikey O'Connor: The thing that cheers me up about this is that this is a sufficient group for a pretty good face to face conversation in Dakar.

Leave your hands up for a moment so that (Natalie) can capture that. And here's the thought that I've had is on the working - on the co-chairs group we've had a conversation about what to do with that meeting.

And the leaning there and I think on a previous call, DSSA call was to make it a working meeting just like the one we had in Singapore. The topic of that work to be determined based on where we are. So the exact kind of work and the agenda isn't determined yet.

But it's not going to be a big public gala, it's going to be another one of these closed meetings just for the working group to do real work kind of meeting.

And I'm working hard on the technology to try and get the workspace working well for people who are coming in remote.

And so I'll probably lead the remote side of the call and one of the other co-chairs will lead the in Dakar.

Okay, so let's see, oh I've gone way behind on my reading. Jacques has a good idea that we should send an email to the mailing list asking people to - (Natalie) maybe you could do that.

Julie Hedlund: Mikey this is Julie Hedlund, I just wanted to point out that it is not a closed session in Dakar.

Mikey O'Connor: Oh it's not? The last one was.

Julie Hedlund: The last one was but this one is open. I think to a certain extent the anticipation was that there would be an update on the work of the group you know at that session, not lengthy.

And I don't think that this means that we can't use that time for you know for the meeting of the group and some substantive work. But it's not currently listed as a closed session.

Mikey O'Connor: Well that's a divergence from my understanding. Maybe we'll take that one up with the co chairs. Why don't we...

Julie Hedlund: That's fine, whatever you decide and we can certainly work with that. It's just that I just wanted to point it out.

Mikey O'Connor: Yes thanks and that's a good catch because it would be bad news if we set up a whole meeting with the anticipation that it was closed and then a bunch of people thundered in and we'd be waving our arms and going what do we do now?

So let's try to remember, circle around to that on the co-chairs call next Monday, see what we can figure out.

Anyway that's kind of what's up there. Then in Dakar there is also a meeting scheduled with the SSR accountability and transparency review team group.

And my memory fails me as to who's invited to that. I think it's everybody in the DSSA is invited to that, but I can't remember.

(Kia): Mikey this is (Kia), definitely everybody in the DSSA is invited, that is a closed session.

Mikey O'Connor: Yes, okay. So for those of you who up till now haven't heard about that, that meeting is I think at 8:00 in the morning on Thursday and we should probably send the note to the email list alerting folks to that as well.

And as I - as we just said everybody's welcome. This is an opportunity for the two working groups to sort of update each other on what they're doing and

we can see if there's any overlap and see if there are ways that we can work together, share information, etcetera.

So it's essentially a working meeting now that we've gotten a bit underway and they're also a bit underway this seemed like a good time to put us all in the same room and see what we can learn from each other.

So Jacques is suggesting a meeting invite with the right time zone for the Dakar meeting. We may - usually the meeting invites go out in UTC Jacques so that people can just translate so wherever they're going to be.

And then it will show up probably in the master schedule for the meeting with the Dakar time listed. Does that sort of cover what you wanted to cover (Greg), is there anything that I missed in that sort of rambling ad hoc not quite prepared - I probably should have done that.

I was kind of planning to do that next week but it's a good idea to get it on people's radar a little bit, his schedule. (Greg) seems to think I did all right.

Okay, if there isn't anything else on Dakar I think I'd like to circle back to the discussion about scope. And hang on a minute while I rejigger my screen here.

First one that oh here it is, all right, trying to find IP, the depletion of the IP V4 address pool. I'm mumbling Cheryl, I'm mumbling, I'm sorry, I'll be there in a minute.

Cheryl Langdon-Orr: Yes you're mumbling and you don't seem to have brought us back to address the question that Jacques has raised in terms of fragmentation of the root.

Mikey O'Connor: Yes and I think what we'll - oh I see, and that one is in scope. All right, so let me just get all that on your screens and I'm close, I'm very close.

And then we can...

Jacques Latour: Because I opened up the - Jacques here, the last version of your Mindjet file and I can't find anything about fragmentation there.

Mikey O'Connor: Yes, here's where it is. It's - this is in the Mindjet file threats, not vulnerabilities. I split this into two because it got so big.

And so in fragmentation of the root, what SAC 9 is talking about is the alternate DNS root, the root scaling kind of stuff that's in SAC 46 and the DNS blocking issues that are raised in SAC 50.

And the group put that one in scope. Do you have an issue with that Jacques? Do we want to move that one back under discussion or do you think that it does fit in scope for what we're doing?

Jacques Latour: No, it's okay. I was on vacation for the last two weeks so I missed a little bit here, so I'm okay.

Mikey O'Connor: Yes well and this is very confusing document that we're working from that's part of the good work that we've been doing is making this easier to follow.

So it's not a problem then, that you couldn't find it in there. We actually have two and this is the last call, the FY12 issue was raised in Singapore. It came in on the results from the brainstorming session there.

And I don't know what that was. I think I'm going to give this one last call and then if nobody can remember what we were talking about I'm just going to take it out of scope.

Is there some event in fiscal year '12 that is coming up, some technical change or standards change or is it just the end of the world which is predicted for when the Mayan calendar runs out?

Maybe that's what it was. Who knows? Mayan calendar, going once, going twice, I might kick this out.

Okay, I'm going to take this out.

Cheryl Langdon-Orr: You crack me up Mikey.

Mikey O'Connor: Well you know the end of the world would be really tough on DNS. Can you imagine the apocalypse, the four horsemen of the apocalypse show up and trash the DNS root servers.

Cheryl Langdon-Orr: Maybe that's the true meaning of it.

Mikey O'Connor: Could be, you know Mayan calendar and the end of DNS. Okay so here's the DNS - the as yet un...

Cheryl Langdon-Orr: I love this, sorry guys.

Mikey O'Connor: I've lost control of the meeting, look at this. Damn you Mayans, damn you. Why do I do this? This is like being in the library and breaking into giggles and not being able to stop, sorry. Okay. Back to work.

Depletion of the IPV4 address pool, the two issues that were raised there were the growth and the routing table and the problems of route - possible route fragmentation problems.

These were raised in SAC 12, (Greg) is snoring. Do you want to expand that (Greg) a little? Are you snoring about the end of the world or are you snoring about fragmentation or depletion.

Cheryl Langdon-Orr: Must be the (unintelligible).

Mikey O'Connor: Everybody's typing, I'll just become your reader again. Mark Kosters is saying this is out of scope. Olivier says I thought IPV4 address pool was the end of the world.

(Rosala) agrees probably with Mark not with Olivier, Jacques says out of scope but he's laughing out loud, oh God. This is out of hand. This does seem to be out of scope. Okay so we need a rationale for it being out of scope folks.

Let me just - we can't put the end of the world on our official - let's see. Okay, let's see, Olivier go ahead.

Olivier Crépin-Leblond: Okay Mikey, as the rationale for it being out of scope I would say that - I would suggest that DNS has never been (unintelligible) consumer of IP addresses so the depletion of IP before address pool is not likely to have much of a significant impact on it. Thank you.

Mikey O'Connor: I think that the issue is more in terms of the routing table which also isn't terribly dependant on DNS so much as just routing.

Olivier Crépin-Leblond: Yes, in either case it's - and in both cases the routing table is going to grow anyway in V6, it's also going to grow. So really it is a non event. Thank you.

Mikey O'Connor: So the rationale is DNS is not a consumer of IP addresses. So changes in the routing table...

Olivier Crépin-Leblond: Mikey Olivier again, it is a consumer, I mean it does use IP addresses, but it's not a heavy consumer.

Mikey O'Connor: Okay, heavy - let's see, let's - why don't you repeat the rest of your rationale, I think actually the other parts were good ones Olivier and I missed them because I'm sort of multitasking here and my darned phone range.

Olivier Crépin-Leblond: Thanks Mikey, Olivier here, I wish I could remember them.

Mikey O'Connor: Well I can pick them up from the transcript too. I'll do it like that. Okay, so out of scope going once, anyone want to put it in scope this is your last chance, otherwise it will go out. Out. And I'll go track down a better rationale.

Okay, now we've got - well we've still got 10 minutes left, let's see if we can pick off another one. Here's another one, we talked a bit about this one and just didn't get done.

What we said about IDN attacks which are look alike characters and so forth for standard exploitation techniques this was coming out of SAC 37 and I think that the payday phrase, this is awfully small, let me make this bigger, the payday in this one is that this certainly isn't in scope in and of itself.

It's more that it could be a threat factor. What we found in the later discussions is that we wanted to put some nuance on some of these that said no, no, no, not in general but that we might want to include them in the discussion of some of the other vulnerabilities as a threat vector.

And I guess the question that we need to resolve is does that make sense for people? Should we include it somewhere as a threat vector or just leave it entirely out of scope?

Let's see, (Jorge) is saying is this - I think Jorge is saying is this ever going to have an impact on the DNS? He's lobbying for out. Then (Greg) says if this one's in then every threat vector is probably in. So I suggest out.

And you know I think whatever, I'm not going to stop being the - Jacques says I have a question, if organization X hosts root - the F root secondary's on their premise, can organization X change the content of the F root of the T root server.

Jacques Latour: No, F root.

Mikey O'Connor: Really F root server, okay. And (Patrick) is saying perhaps it should be change from attacks to management of confusable strings. This one could be changed from an attack to what?

(Patrick) go ahead.

(Patrick): Yes, Mikey it's (Patrick), so in looking at this if the issue is about look alike characters and confusability, I mean this is going to touch on something that is...

Mikey O'Connor: (Patrick) I'm going to interrupt you and encourage you to get a little closer to your phone.

(Patrick): Let me take it off speaker. So this one is I think related to some of the ongoing work within the variant project. And how strings that involve confusable characters may be managed or not. It's a whole 'nother category that's not under attacks.

So you might want to sort of break this off from where it is and change the focus, but - and maybe (Greg) or somebody else can add to it, but I would take it out of this area but preserve some discussion for management of - or dealing with strings and IDNs in a way that may actually have an operational impact.

Mikey O'Connor: (Greg) is saying are we talking about variance of TLD strings or at the second level and below? I think just winging it here (Greg) I think that at least when I put this in and wrote this stuff I was thinking it was TLD strings only.

But anything at the second level and (Patrick) is agreeing, anything at the second level is out of scope for sure. Then the question would be if you had a variant of a TLD string how would it ever get routed to?

I think (Jim) Galvin is saying I think we should at least leave this as an under discussion until we can see what the results of the ICANN variant case study work is.

(Patrick)'s agreeing with (Jim) on that, (Greg) has pasted a link to - Cheryl go ahead, fair point?

Cheryl Langdon-Orr: No, I'm mumbling. I'm doing a you, don't worry about it.

Mikey O'Connor: Okay that's fine, you know mumbling is a good contagion. So I'm pleased to see - you know maybe by the end of this working group we'll all be sort of stumbling, mumbling lurching about type people.

Okay so it sounds like at least leave it under discussion, find a better home for it, maybe make sure that it's - (Greg) just clarified the link that he posted, the variant project says "the benefits and risks associated with the potential delegation of variant TLDs."

(Patrick)'s saying take out the attacks, yes, I've got that in there. So why don't I take an action to find a better home for it. And we'll leave it under discussion.

And we're going to - oh and (Greg) is that the link that you posted is to the variance project page? Okay, thank you very much sir, (Greg) says yes for the transcript, paste that in.

Okay, good deal. All right, I'll take an action to fiddle with that a bit. Okay, the next one that's still under discussion is malicious or unintentional erroneous alteration of DNS configuration in SAC 44.

And this again is the - there's a pile of stuff, let me see if I can thin that out a little bit. SAC 44 was a pretty broad conversation about names server configuration information and clearly in general this is out of scope for us.

Because if we put this all in scope we'd be all the way down to the very edge of the network and that's not our intent. So the conversation we had on scope was - is summarized here.

And what we were saying when we talked about it was it clearly depends on the target and if the target were at either root or TLD level it might be also depends a bit on the number of domains that are affected.

I think that's again clarifying that we're really only talking about root and TLD level. And then if we were to explore this we would have to clarify this narrowing of the scope.

No we're not going to tackle everything that's in SAC 44, but to the extent that it's directed at or an issue at the root or TLD with that caveat is it in or out of scope, I think that's the key.

And Cheryl typed in the chat I'd leave this one under discussion noting the limitation to the root and the TLDs and we could certainly do that too.

Or we could just agree that at the top level in TLDs this is in scope. Is there anybody that disagrees with that?

Cheryl Langdon-Orr: Okay, Cheryl here for the record, I don't disagree with that, I'm happy with it to be in scope but if it's in scope I think what needs to be decoupled

specifically from SAC 44 unless we're really clear about the limitations to TLD.

Because SAC 44 is so general. Does that make sense?

Mikey O'Connor: Yep.

Cheryl Langdon-Orr: Okay.

Mikey O'Connor: How about that for a refinement?

Cheryl Langdon-Orr: That I can live with in scope.

Mikey O'Connor: Okay so if we did that, let me just refine that a little bit to get that in there, how do people feel about that revised version? (Jim) is typing and I think we'll kind of wrap it up after this last little discussion.

So if we don't get the conclusion we'll just leave it under discussion and wrap up for the day. Yes, (Jim)'s way ahead of me.

Yes, we're going to wrap up real soon. Let me leave it under discussion for now and we'll circle back to this one. It is the top of the hour and I thank you all for another great conversation today and see you in a week. Bye bye.

Cheryl Langdon-Orr: Thanks Mikey.

Woman: Bye, thanks.

Man: Thanks bye.

Coordinator: Thank you sir, you may now stop the recording.

Woman: Thank you.

Woman: Thanks (Natalie) a million, it sounds like we're all set and...

END