Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
15 September 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 15 September 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-20110915-en.mp3

Transcript will be posted shortly on:
http://gnso.icann.org/calendar/#sep

Attendees:

Greg Aaron, GNSO
Sean Copeland, ccNSO
Keith Drazek, GNSO
Mark Kosters, NRO (co-Chair)
Cheryl Langdon-Orr, ALAC
Jaques Latour, ccNSO
Takayasu Matsuura, ccNSO
Rossella Mattioli, GNSO
Mike O'connor, GNSO (co-Chair)
Arturo Servin, NRO
Carlos Martinez, LACNIC

ICANN Staff:

Bart Boswinkel
Julie Hedlund
Gisella Gruber

Apologies:

Luis Diego Espinoza, .cr
Olivier Crepin-Leblonde, ALAC (co-Chair)
Jim Galvin, SSAC
Jörg Schweiger, ccNSO (co-Chair)
Scott McCormick, GNSO
Roy Arends, ccNSO
Don Blumenthal, GNSO
Wim Degezelle, CENTR
Nishal Goburdhan, NRO
Subramanian Moonesamy, NRO
Katrina Sataki, ccNSO
Patrick Vande Walle, At-Large

Patrick Jones, ICANN Staff

Coordinator: The call is now recorded. Please go ahead.

Gisela Gruber-White: Thank you. Good morning, good afternoon, good evening to everyone. On today's DSSA Working Group call on Thursday the 15th of September we have Cheryl Langdon-Orr, Mike O'Connor, Sean Copeland, Takayasu Matsuura, Greg Aaron, Jacques Latour. And on the Adobe Connect we have Mark Kosters, Rosella Mattioli as well. And from staff we have Bart Boswinkel, Julie Hedlund and myself Gisela Gruber.

Regrets today we have from Jim Galvin, Patrick Vande Walle, John Levine, Wim Degezelle, Luis Diego Espinoza, Olivier Crepin-LeBlond, Joerg Schweiger, Scott McCormick, Subramanian Moonesamy, Katrina Sataki. I hope I haven't left anyone off the list. And if I can please remind you to state your names when speaking for transcript purposes. Thank you. Over to you Mikey.

Bart Boswinkel: So Gisela, this is Bart. And we just received one from - an apology from Roy Arends as well.

Gisela Gruber-White: Lovely. Thank you.

Mikey O'Connor: And Greg Aaron and Keith Drasek both just jumped into the Adobe room, so I imagine that they'll be joining the call shortly. Welcome. And one last logistical note. The Internet connection her at the farm is pretty unreliable today. So I may drop out of the Adobe room in which case - Mark, are you on the call? No. He's just...

Cheryl Langdon-Orr: No he's not.

Mikey O'Connor: Okay. Trying to find me a co-chair that I can throw the ball to if I fall off Adobe. We'll just keep our fingers crossed. Sounds like I'm the only co-chair on the call.

Well, our agenda is identical to last week. I apologize for not publishing it. I have been having a lot of connectivity issues and didn't get the mail out. Sorry.

So anyway, we're going to do exactly the same thing. What I've got up on the chat room right now is a reminder for you all of Greg's proposed refinement to the scope conversation which we discussed last week on the call - continued discussing a bit on the email list with my clearly out of scope example.

And what we are - we've invoked sort of the two meeting rule on Greg's scope email. And this is our second meeting. If - I think what we'll be is a little bit flexible on this two meeting thing because we've got so many people missing the call today.

We may - I think what I'd like to do if it's okay with the rest of you is defer the consensus call on this until next week's call. Presumably we'll have more people on the call.

Woman: Great.

Mikey O'Connor: Feels a little odd to do the second consensus call on this today given how sparse the attendance is.

Bart Boswinkel: Mikey, this is Bart.

Mikey O'Connor: Yes. Go ahead.

Bart Boswinkel: Yes. May I suggest that you send out an email to the - to make it clear, I can do it as well, but so everybody's aware this is happening.

Mikey O'Connor: Yeah. I will do that. That's a good idea. I'll just start taking my little to do list notes here so that I don't forget. Because I don't want to get to the point where we get stuck because we don't have enough people on calls to do the consensus stuff.

I suppose another way to do it would be to go ahead and treat this as the second consensus call and then that might serve as a pretty pointed example of why it's a good idea to make all the calls. I think I feel a little uncomfortable doing that. So let's wait a week and I'll send a note like you said Bart.

So with that, what I'd like to do is go back to the - clear this note out of here. I have to do a little - fiddle around with Adobe for a second while I share the document that we're working on. As I say, it takes a lot of clicks to do that.

It looks okay from here. I'm going to move us on to sort of the next chunk because I think we might have a pretty lively discussion about this. This is a pretty un-stratified list right now. And what I'd like to do is see if we could get through the direct attacks list today at least tentatively with our in or out of scope discussion.

And, you know, right at the top of the list I think is one that's in scope. We have a ton of information about it. I don't want to - the reason that I'm building such a detailed tree is because when we take one that's in scope like this DDoS one, I think that detailed tree will be helpful to the people who decide to do - to participate in the analysis of any given thing.

So panic not. We're not going to write a report with all that stuff in it but I'm using this as a way to sort of assemble some background materials for the groups that are going to work on this.

But if we start with DDoS, I'm assuming that that one is in scope. Anybody want to challenge that notion? And if not - don't you like my crayons. I think they're just cute as a bug. Going to put that one in scope.

Now the next one, packet interception, is one I'd like to discuss. I don't know. How do people feel about this one? And this is a direct attack against the DNS. There are certainly lots of packet interception attacks but I'm not sure whether this is one that we need to deal with.

And I'm seeing Carlos come in. Lots of people coming in. I saw - oh Mark and Jacques wants in. Mark and - so the works for me from Mark, was that for leaving it in or out? Is that - are we talking - the trouble with chat is that it's hard for me to keep track of it. So I don't know where we're at in the discussion.

Why doesn't somebody do the raise the hand thing so that I can? Oh, okay. Arturo is - Mark, are you - oh, you're stuck too because you're only able to listen. No mike either. So tell you what. If - given the - given that difficulty, why don't we use the thumbs up/thumbs down capability?

So if you go up on top of your screen, right in the middle of the screen is a little outline of a person raising their hand. And if you click the little gizmo next to it, you can see that you can agree or disagree. And so what we're agreeing or disagreeing about is whether this is in scope - if you think this should be in scope, give us a thumbs up. And carry on from there.

I'm seeing some thumbs up and a raised hand. Sean, are you...

Sean Copeland: Oh, sorry, was that - okay. That was my fault. I wanted to do a thumbs up. I apologize.

Mikey O'Connor: That's okay. I'm big on learning how this works, so mistakes are just fine. It looks like in scope is the way we're going. So if anybody wants to lobby hard

for out of scope, this is your chance. Otherwise I'll put it in scope. Okay. In scope it is. Have to relearn how to do this. There.

All right. Let's just keep going on this theme. Will - so everybody clear your little thumb by going back up to that thing in the middle and just at the bottom there's a place where you can clear your status. So go ahead and clear your (unintelligible) - there we go.

All right. So now we're doing recursive versus authoritative name server attacks. In or out of scope, thumbs up/thumbs down. Rosella's got it in. Jacques' got it in. Cheryl's got it in. Mark's got it in. Sean's got it in. Okay. (Name) deal. We'll just - I think this is a good way to do it unless people get uncomfortable. If you get uncomfortable, let me know and I'll either slow down or change the way we're doing this. But seems to be going well.

Okay. Everybody clear your status. This next one is for authority or authentication compromise. This came from Singapore. And again, I think it would probably be safe to say that this is a compromise of a registry or a registrar. Again, thumbs up or thumbs down. I'm seeing thumbs up.

The way this is going maybe what we should do is just look at this list and see if there are any that we want to take out of scope. That will - still kind of learning what I'm doing here. Dagnabbit. There.

Ah. Well here's a perfect example. So domain name hijacking and theft. That seems like a tasty one. Is that in or out of scope? Mark. Mark's got his hand raised. Oh, thumbs up. In scope. All right. Greg has got it out of scope. I though you might. Jacques, is that a hand - a thumbs up but missed or do you want to speak? Carlos has got it in scope. Let's have a little debate about this.

Jacques Latour: It's Jacques here.

Mikey O'Connor: Yeah. Go ahead Jacques.

Jacques Latour: So we're talking about a specific domain name hijacking or a bunch?

Mikey O'Connor: I think that was SAC 7 is -- well, there's not a whole lot in that little tab -- is the...

Jacques Latour: One domain.

Mikey O'Connor: Yeah. I think that this is the act of hijacking or theft. And so it's not - it's - one of the things that we've been talking about is using something as an attack vector against registries and registrars. And this...

Jacques Latour: So.

Mikey O'Connor: ...is not that. This is the broader case.

Jacques Latour: So the one before like if you have (unintelligible) come from (unintelligible) then you have potentially all the domains are hijacked.

Mikey O'Connor: Correct.

Jacques Latour: So that bullet refers to just one, so out.

Mikey O'Connor: Yeah. I think that's right. And I think that's probably the reason that Greg is suggesting out of scope. So is Jacques. So is Arturo. Mark and Carlos are for in scope. Rosella is for out of scope. Let's talk to Carlos about why he would like to see it in scope. It's - oh, Cheryl, is your hand up? Do you want to speak? I'm sorry.

Cheryl Langdon-Orr: Yeah. Just briefly. Cheryl for the transcript record. I just think that when we get to an individual domain name it has nothing to do with security and stability. It's out of scope. I was fence sitting but I needed to say to you all I'm

probably leaning towards the out of scope side of the fence rather than anything even vaguely perpendicular.

Mikey O'Connor: Right. So I'm going to put some scope notes because I think this one's leaning towards out of scope.

Cheryl Langdon-Orr: If it's - Carlos is just raising mass - Cheryl for the record. Carol is raising mass hijacking. That's a different story to me.

Mikey O'Connor: Yeah.

Cheryl Langdon-Orr: I think we almost need this a little bit more specifically delineated in exactly what it means; if it's individual or limited number or domain hijacking, then it's not in scope. But if it gets to be seriously large numbers, then that might be another issue.

Mikey O'Connor: Well and it may be that - I think the example that we were using is if - so if I - if you could take a look at that little scope thing that I just wrote, does that sort of capture the thought that we've got here is the domain name hijacking especially at the individual domain level is out of scope. But that maybe if a lot of them were hijacked would be something we want to consider but that's probably best considered under the topic of how they did that mass hijacking.

I mean hijacking within the registry is out. Hijacking via network or via protocol is in. Could we then - Jacques, this is for you. If we could then - yeah. And there's Greg coming in. A mass hijack due to compromise of a registry equals authority compromise.

So it sounds...

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: ...like the way to handle this is to take this one out of scope and then address it however the mass hijacking was accomplished either via the network or via authority compromise. Let Jacques finish typing and then presuming that he's agreeing with that approach, yeah, see then Jacques, I think what we would say is packet interception is in scope perhaps as an attack vector. But that the hijacking is almost an artifact of the thing rather than the breadth.

Cheryl's off the fence. I think we're going to take this one out of scope. Last call on this one. Okay. Going once, going twice, here goes the - ooh. Just went dark. There that's better. I like that.

Okay. Registrar impersonation phishing attacks. There's quite a lot about this. And the thing out of the SAC 28 report was - really this is the one by impersonating a registrar the capturing registrant credentials through phishing attacks. How do we feel about this one? Is it in scope or out of scope?

Greg's got it out. Arturo's got it out. Another one for Cheryl is saying (hm), so out for Cheryl. Okay. We're starting to see an early trend towards out of scope. Sean has got it out. Now Rosella's got a (hm) there.

Well we could capture that as a - who else would expose this Mark? Who else - you mean what other working group Mark? If we don't - in other words if we don't do it, then who else would do it? Oh. Getting a lot of out of scopes.

Well it wouldn't be quite the same as - Jacques is submitting an authority compromise as a way out. This - I'm not sure. Well yeah, it would be an authority compromise in this case of the registrant. That's true.

Cheryl Langdon-Orr: Yeah.

Mikey O'Connor: That's the way to handle this.

Cheryl Langdon-Orr: Yeah. That'd cover it.

Mikey O'Connor: Okay. (Unintelligible).

Jacques Latour: Jacques here.

Mikey O'Connor: Pardon me. Go ahead.

Jacques Latour: So if somebody takes a registrar credential like the super user account...

Mikey O'Connor: Yeah.

Jacques Latour: ...then the registry or the registrar is compromised.

Mikey O'Connor: Right. This could be addressed as a authority - leave it like that. And I think that's the way back in Mark to your point. But we could raise it as a form of authority compromise. Put that in. That's not a very good word. Let's do that word instead. How about that?

Okay. Quick bunch of buttons. Okay. Next one. Data poisoning. There's a bunch of stuff under here. RFC 3833 talked about it in terms of the DNSSEC. There's the (Kaminski) stuff, the (Caspera) stuff. Greg's got that one out of scope still. Lots of in scope on that one.

Cheryl Langdon-Orr: Okay Greg. Tell us why.

Mikey O'Connor: Yeah Greg.

Cheryl Langdon-Orr: Calling Greg.

Mikey O'Connor: That might be an old hand. He's now - ooh, that's a neat symbol. He's got sort of this peculiar dash symbol in there. Speak to us Greg.

Cheryl Langdon-Orr: He's stepping away.

Mikey O'Connor: Oh he's stepping away. Coward.

Cheryl Langdon-Orr: He's running away after that one I think.

Mikey O'Connor: All right. All right. Well let's see. I think we're getting pretty good in scope on this one except for Greg peculiar behavior. All right, we're going to put it in scope and then let Greg howl if he wants to.

Cheryl Langdon-Orr: Oh I think he was affected by lag time.

Mikey O'Connor: I see. Okay. Okay. So I click away here. Oops. All right. Footprinting. What's footprinting? Oh, this was out of Microsoft. I was going wild there for a while on the Google search. So what do people think of footprinting?

This is the process of building a diagram or a footprint of a DNS infrastructure by capturing DNS zone data such as domain names, computer names and IP addresses for sensitive network resources. DNS domain and computer names often indicate the function or location of domains and computers.

Cheryl, go ahead.

Cheryl Langdon-Orr: I was a little confused about what this meant. So we've - my declaring absolute naivety and only giving you a knee jerk reaction on what that limited example of explanation is, I will say in scope. But I've not understood it. I have not delved into it. I have not analyzed it. And I claim no understanding of it in any way (unintelligible) wise.

So, you know, it looks like it should be in scope but that is purely knee jerk and I need to make that a clear declaration.

Mikey O'Connor: Great disclaimer. I think that gets the disclaimer of the day award. Greg, go ahead.

Greg Aaron: I can't recall who had suggested this one but what it sounds like to me the kind of thing that for example hackers do. They scan networks to find machines, open ports, operating systems, boxes using that kind of a thing. I mean it's a behavior or a threat vector. But I don't understand how this qualifies as a threat to the DNS. It's just a behavior which can be in some cases bad, in some cases not.

Cheryl Langdon-Orr: Mikey how can I put my hand up? My screen is grayed out. Do you know?

Mikey O'Connor: Oh, I think you have to choose.

Cheryl Langdon-Orr: Oh well, I'm clearing my gray temporarily. Just as a follow-up Cheryl for the record, this is a follow-up Greg or Jacques can you help me understand why that is not a threat to security or stability because I'm happy to come off my, you know, knee jerk reaction if I understand a little bit more.

Greg Aaron: This is Greg. It's a threat to the security or stability of individual machines or systems but I haven't heard yet how it's a threat to the DNS.

Cheryl Langdon-Orr: Okay, so it's a fairly focused and limited effect. It's not what we would - I guess roughly define as a widespread or numerous machine effect?

Jacques Latour: So -- this is Jacques -- so my internet work I'm trying to protect from that. I don't want people to know what I have inside.

Cheryl Langdon-Orr: Yes.

Jacques Latour: Or my financial systems are and all that stuff. So I'm trying...

Cheryl Langdon-Orr: Yes.

Jacques Latour: This is information we hide and footprint things is a technique to discovery your internal infrastructure.

Cheryl Langdon-Orr: Okay.

Jacques Latour: And what you published is on file for dot.com then, you know, its all there. It's not a trip or that.

Cheryl Langdon-Orr: So it's a very narrow focus (effector)?

Jacques Latour: (Unintelligible) price.

Cheryl Langdon-Orr: Yes, it's a very narrow focus. Okay.

Mikey O'Connor: It falls in the category of a means to do something else that's in scope. So it might be a means to compromise critical resources but it's not a threat in and of itself.

I think it's just falling in that ever growing category of attack vectors or mechanisms through the - mechanisms rather than threats, that's sort of where we're headed with this?

Who put this one out of scope? I may have just found this one people so, you know, don't -- I'm not sure that this is one that necessarily has any credibility at all.

(Fastflux), I think I can predict that Greg - I can predict that Greg Aaron's going to give us the thumbs down. Greg and I spent a lot of time together talking about this one.

Greg Aaron: I earned that right by spending a year on a working group on that very topic.

Mikey O'Connor: Indeed you did. And I was the chair of that working group for the first half of that painful year until I flamed out and let James Bladel carry the football over the goal line. So I will join Greg in giving that one a thumbs down.

Again, it's a mechanism in some cases but that's it.

Cheryl Langdon-Orr: Got my hand up Mikey.

Mikey O'Connor: Oh, I'm sorry, go ahead Cheryl.

Cheryl Langdon-Orr: Thank you. Cheryl Langdon-Orr for the record. Based on our previous discussion and my education thank you gentlemen, I would suggest that once I'm a card carrying fan of (Fastflux) things store if possible. It is not I would therefore assume if we're using those prior definitions and if I'm saying this as a small focus affect not a generic effect for the security that's similar to the (unintelligible) something that is in scope.

Is that a fair and reasonable knee jerk reaction from a point of view? Because I'm - if it's only just a few, you know.

Greg Aaron: It's a -- this is Greg -- yes, it's used to facilitate other things like, you know, hosting the website or...

Cheryl Langdon-Orr: Yes.

Greg Aaron: ...its spam and, you know, things like that. And the by the way the numbers are not significant either - the number of domains being posted this way in comparison to the world of domains.

Cheryl Langdon-Orr: But it's not exactly threatening the security civility of the DNS?

Greg Aaron: It is not in my opinion and that was the general consensus in the GNSO working group. So that's it.

Cheryl Langdon-Orr: Okay. Thank you.

Mikey O'Connor: Okay, last call before we place this one out of scope. Oh, there's a bunch going on in the chat. Carlos is saying (Fastflux) is deployed as an invasion technique but very similar techniques are sometimes legitimately deployed by CDNs for example.

So it's more a question of intent rather than a threat as Marcella agrees there. I think we've got a pretty good consensus with that one out of scope. Okay, IDN attacks, we'll go through.

Cheryl Langdon-Orr: My status is, you know, getting a clear status.

Mikey O'Connor: Yes, well, I wouldn't want that. On to IDN. Oh, you want to speak?

Cheryl Langdon-Orr: No, no it went to -- all I wanted to do is clear and it's gone silly. Gee.

Mikey O'Connor: I'm trying to help you. There we go, now it's off. Okay, IDN attacks, look like characters, etc. for standard exploitation techniques. This is the display and use of internationalized registration data support from characters from local languages or scripts.

And its SAC report 37 is about this, Greg's got his hand up, go ahead.

Greg Aaron: This is an issue of confusability. It's also an issue of individual domain names for the most part. I think what we're talking about here are from a demographic attacks. Is that correct?

Mikey O'Connor: I think that's right.

Greg Aaron: Okay. And it's more of a theoretical usage than an actual usage. (Unintelligible) and I practiced for the anti-phishing working group. There

have been two confirmed domain names of this type in the last three or four years. It's definitely out of scope for me.

Mikey O'Connor: Okay.

Greg Aaron: For those reasons.

Mikey O'Connor: We'll give it the same standard justification. I'm using this scope to sort of mostly justify the reason we're taking things out of scope so that we can document that.

(Rosella) do you want to have -- are you saying that this is in scope? (Rosella)'s typing, we'll pause for a minute for (Rosella)'s to us via the chat and chat is getting ready to explode.

(Rosella) said we should at least consider as a marginal threat that could be largely exploited in the future. We could do that or we could put it in our Attack vector pile, that's primarily what people are trying to do with this.

Carlos says, "My concern here is on possible software bugs dealing with IDN string processing." Cheryl is on the fence.

Cheryl Langdon-Orr: I want it parked.

Mikey O'Connor: Or parked. Yes, well we could park it. If we leave it uncolored, not green, not red, then that means that it's for further discussion. All right, I'm getting some enthusiasm for parking this. Okay.

Cheryl Langdon-Orr: Like it's something we have the data yet.

Mikey O'Connor: Yes, let's - let's -- if we're on the fence, there's no reason especially on a lightly attended call to plunge ahead. We don't have many parked items so it's not going slow us way down if we have a few more.

So Greg are you okay if we park this one?

Greg Aaron: I feel pretty strongly it's a matter of individual domain names. So, you know, if you want to park it I mean...

Mikey O'Connor: I think we better park it. We'll have a focus discussion about this. We can do a little prep work and stuff like that. Okay. Next one is authenticated denial of domain names. This one is RFC-3833 and they -- I did a very bad job of summarizing this.

This was very early in my summarizing career. I apologize for this. I'm going to try and remember what this was about. It had to do with an authenticating the non-existence of a name. And I think this was all to do with their discussion of DNS SAC.

And we may have to park this one because my memory is so lame as to what the actual situation was. Cheryl, go ahead.

Cheryl Langdon-Orr: Thank you. I may need a disclaimer and please explain thing for the call. Correct me if I'm wrong but if we're talking about single or limited numbers of names. I don't understand how it could be a threat to the DNS security or stability.

Mikey O'Connor: Oh, that's a good point and it was definitely that. It was an error either...

Cheryl Langdon-Orr: In which case I'd be giving it a thumbs down.

Mikey O'Connor: Yes, I think that's true we could certainly use that to stand on. It's not a widespread attack. All right, I can live with taking that one out of scope. Let me use my handy-dandy scope deal.

All right. All right.

Cheryl Langdon-Orr: Clear, clear, got to clear. It is on clear it puts my hand up. Sorry.

Mikey O'Connor: It just knows - it just knows you so well. It's not going to go there.

Cheryl Langdon-Orr: I just like talking to you Mikey. It's not to Mikey.

Mikey O'Connor: Oh, my goodness. Look at all those, there's a boat load, let me thin this out a little bit so I can see what the dickens we're talking about. Oh, this was all down, gracias.

Cheryl Langdon-Orr: I'm getting dizzy just watching the screen Mikey.

Mikey O'Connor: Sorry, I didn't pre- I didn't prevent this. Okay, so this is - I think this is the mechanism to gain control of a gained authority. So this is one we can handle a different couple of ways.

Cheryl Langdon-Orr: I'm going to put my hand up here.

Mikey O'Connor: All right, go ahead. Cheryl for the record.

Cheryl Langdon-Orr: Cheryl for the record and my response to this would be different if we talking about registry, registrar, registrant.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: So I can't deal with this one while those targets are bundled.

Mikey O'Connor: All right. So well, what we could do is we could tentatively take registrant out of scope.

Cheryl Langdon-Orr: Yes, I'm happy with that.

Mikey O'Connor: Put registry and registrar in scope, how about that?

Cheryl Langdon-Orr: Well, that would be my view, but I don't know about everyone else's.

Mikey O'Connor: Well, if we did that caveat let's see some - see some thumbs up and thumbs down action on the list there. People are pondering this. The mitigation then is...

Cheryl Langdon-Orr: Yes, I think...

Mikey O'Connor: is out of scope because that's a registrant attack.

Cheryl Langdon-Orr: Yes, that's - they...

Mikey O'Connor: Yikes, sorry.

Cheryl Langdon-Orr: They're interwoven where I'm not sure they should be the way that mine's been done.

Mikey O'Connor: Yes. And so what we'll do is we'll do this.

Cheryl Langdon-Orr: And yes, I agree with Jacques it really could be defined under authorization, couldn't say the word.

Mikey O'Connor: Right. All right, so let's do a scope today. Let's -- I mean we could use these same - the same rationale that we've been using all along which is...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: ...that this is an attack vector and certainly if it were against a registry or registrar especially a registry...

Cheryl Langdon-Orr: Then it's an authorization issue.

Mikey O'Connor: ...it would be pretty catastrophic but...

Cheryl Langdon-Orr: But it's also an authorization issue.

Mikey O'Connor: Right. So I'm not hearing anybody lobbying hard for in scope. Because this is your last chance to lobby for in scope, otherwise it's going to be...

Cheryl Langdon-Orr: They could have been an example of in the authority compromise section. So I intended to move all of that discussion space up as one of the exemplary under the...

Mikey O'Connor: Sorry to -- all right, let's do that right now. This will take a second because that's a giant tree under there. It's going to take a second to push all that under there, but it's my little -- as you can see -- my little...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: ...computer working hard to do that.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: And then what we'll do is we'll make this example and we've got our registrant out of scope that. Sorry to destroy your eyes. Look away from your screen for a minute so that I don't give you an epileptic fit. This one is in gone. All right.

Cheryl Langdon-Orr: Good.

Mikey O'Connor: Excellent. Malicious or unintentional alteration of DNS configuration information as is described in SAC-44. I apologize in advance, this may explode your screen too -- it did.

Sorry, there's a lot of mitigation, but there's the description from SAC-44. Maliciously introduce changes to the DNS domain name server to the configuration information associated with a) domain name - a result of the domain name result of the IP address other than the address registrant tended, starting to look pretty individual, naming pretty registrantee.

Such changes can result in the loss of disruption of the registrant's services, etc. etc., and given the theme that we're on -- oh, we've got some in scope on this one tendency coming from the group. Cheryl, go ahead.

Cheryl Langdon-Orr: Thank you, Cheryl for the record. This is another one of those if it's affecting a number, a larger or significant number, then yes it's in scope. And if it's a malicious or - malicious is probably going to be more than just, you know, one or two names.

But if it's, you know, down to one name or more even a hundred names or even more than that's probably not going to affect the stability and security of the DNS. So I'm one of those it depends on the focus narrow or wide.

Mikey O'Connor: So we've got thumbs up saying it's in scope. Greg is pointing out correctly that SAC-44 is a registrant's guide to protecting domain name registration accounts. You've gotten that one, yes, and so I think I put this in not so much because of the registrant perspective, because I agree there.

But from the perspective of if this was done through at either the registrar or the registry level, Greg is pointing out this is an individual domain name issue or a group.

So if - let's so Greg what if -- let's take a ICANN participant with a lot of domain names like VeriSign or Verizon. And they had their DNS name server changed across all of VeriSign's domains, that's still at the - it's still at the domain the sub-domain level rather than the top-level domain level which is

really our focus. Greg is saying not an ICANN issue. It's not a threat to the DNS.

I get that. So for those of you who've got your thumbs up saying that this is in scope let's hear some rationale as to why this is in? I would tend to follow Greg's lead on this one.

Cheryl Langdon-Orr: I think Jacques should speak. I think (unintelligible).

Mikey O'Connor: Yes, that probably is a clue. Go ahead Jacques.

Jacques Latour: I got - so the issue here - do you can hear me clear now?

Mikey O'Connor: Yes, I can hear you fine.

Jacques Latour: Okay. So DNS SAC wise when you think about that so for registrar changes all the keys by mistake and that they're invalid. So that's a stability issue large scale.

Mikey O'Connor: Right. Yes, I think that maybe the thing to do is...I think the mistake that I made is that I used an example that's out of scope. But the example that Jacques just gave is an in scope example of all, you know, if we were to say.

Cheryl Langdon-Orr: Yes, good idea Jacques park it.

Mikey O'Connor: Park, good plan. I like that. Okay. Malicious -- this is the same thing, the same exact issue and I think we're going to leave it. This might be a better example of the one that Greg is talking about where this is really all individual domain name related. I'm going to just do a note here.

So how's this one, in, we've got a couple outs. Anybody want this one in, this is actually a much cleaner example of the point that Greg is raising, much

more narrowly focused. I'm seeing this one going out of scope and I would agree. Good.

So out of scope for the same reasons and look at my little gismo and call that out of scope and noting that it's five minutes before the top of the hour. I think that this is a good stopping point.

We've covered another big chunk of direct attacks today. There's no way we're going to get through the next chunk, that's too big. So I think we'll call this the end of this call and thanks to all.

And we'll see you in a week.

Cheryl Langdon-Orr: Thanks Mikey.

Jacques Latour: Thanks Mikey.

Greg Aaron: Thanks.

Woman: Thanks.

Man: Bye, bye.

Woman: Thanks everyone.

Woman: Thanks have a good one.

Man: Bye.

END