Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
11 August 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 11 August 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-20110811-en.mp3

On page: http://gnso.icann.org/calendar/#aug
(transcripts and recordings are found on the calendar page)

Attendees on today's call:
At Large Members
Olivier Crépin-Leblond
Cheryl Langdon-Orr
John R. Levine
Andre Thompson
Edmon Chung

ccNSO Members
Ondrej Filip, .cz
Luis Diego Espinoza, .cr
Takayasu Matsuura, .jp
Jörg Schweiger, .de (co-chair)
Chris Wright, .au

GNSO Members
Don Blumenthal – (RySG)
Rossella Mattioli – (NCSG) - Adobe Connect only
Mikey O'Connor – (CBUC) (co-chair)
Adam Palmer – (CBUC)
Rafik Dammak, GNSO

NRO Members
Andrew de la Haye - Adobe Connect only

SSAC
ICANN Staff: Bart Boswinkel – Adobe Connect
Patrick Jones
Glen de Saint Géry

Apologies:
Greg Aaron – (RySG)
Ondrej Filip, .cz
Wim Degezelle, CENTR
Jim Galvin
Mark Kosters
Katrina Sataki, .lv
Sean Copeland, .vi
Richard Wilhelm
Julie Hedlund

Coordinator: We're now recording.

Glen de Saint Géry: Thank you. Good morning, good afternoon, good evening everyone. This is the DSSA call on the 11th of August. And on the line we have Rafik Dammak, Cheryl Langdon-Orr, Mikey O'Connor, Eric Brunner-Williams, Adam Palmer, Takayasu Matsuura, Don Blumenthal, Olivier Crépin-Leblond. And on the Adobe Connect we have Rosella Mattioli and Andrew de La Haye. I believe they are just going to be on Adobe Connect.

And for staff we have Bart Boswinkel who is also on Adobe Connect who will not be on the call itself, Patrick Jones and myself, Glen de Saint Géry. Have I left off anybody? And for apologies - for those who cannot be on the call today we have apologies from Jim Galvin, Ondrej Filip, Mark Kosters, Wim Degezelle, Katrina Sataki, Richard Wilhelm. And Bart says he can only be on the call for half of it because he has a conflict with another call.

Thank you, Mikey, over to you.

Mikey O'Connor: Thanks a lot Glen and welcome everybody to the call today. We'll just do our usual thing and take a quick moment to check and see if anybody wants to alert us to a change in their status in terms of their statement of interest.

Okay today we're going to continue summarizing the Singapore work. And so what you see on the screen is the - oh and if folks could mute their phones when they're not speaking. We haven enough people on the call it will get background noise otherwise.

Anyway for those of you who have been through this before this is the summary of the charts that we prepared in Singapore in what's called (mined) mapping format. And what we'll do I think today is just see if we can clump these together. Our habit is to sort of go group by group and let them summarize their work.

And - has everybody got a black screen or is Eric...

Cheryl Langdon-Orr: I've got a black screen, yes.

Mikey O'Connor: Well that's a pain in the neck. Hang on a minute; let me see if I can get that fixed. Oh I see what happened, all right. How about now? Better?

Cheryl Langdon-Orr: Not yet.

Mikey O'Connor: But...

Cheryl Langdon-Orr: We can see your little mouse wandering around we just don't see anything else.

Eric Brunner-Williams: I've got the email list. There we go.

Mikey O'Connor: How about that?

Cheryl Langdon-Orr: Hey...

((Crosstalk))

Mikey O'Connor: There we go. Sorry. Thank you, Eric.

Cheryl Langdon-Orr: That did it. Let there be light.

Mikey O'Connor: Let there be light. Good thing that Eric...

Cheryl Langdon-Orr: ...and emails.

((Crosstalk))

Mikey O'Connor: ...posted that into the chat for us so there we go. All right so now - now we can see - I could see it fine on my screen; I don't know what the problem for the rest of you was. Actually I do, sorry about that.

Anyway so it's kind of an eye chart right now. I'm going to make it a little bit bigger as we concentrate on the individual ones. And I was curious if anybody wanted to go first. It looks like we have Katrina, Roy, Mark, Olivier and - who did we decide our question mark person was? Was that maybe - anyway we'll go through these one by one.

And I think that the goal today is mostly to put these in some sort of a taxonomy and begin to compress out the duplicates. And it clearly will take us several calls to get through this so I'm not feeling any urgency to get through the whole thing.

Let's see, Mark, are you on the call today? No he has regrets I think. Well let's start with Mark's anyway. A little bigger.

Glen de Saint Géry: Mikey, Mark has sent his regrets.

Mikey O'Connor: Yes, I just saw that. Oh there's a spectacular echo. Is everybody getting a 5-second echo like that? Once again, everybody, if we could make sure that we're muting our speakers on our computers, maybe mute your telephone lines too if you can. I don't know, 5-seconds is quite a long delay. I don't know quite how that's happening.

Anyway Mark's group was the group of people that were on the phone. Oh this is driving me crazy.

Cheryl Langdon-Orr: Somebody must have their - it's Cheryl here. Someone must have their - the speakers on their computer on as well.

Mikey O'Connor: Yes.

Cheryl Langdon-Orr: That's the only answer for that sort of thing I think.

Mikey O'Connor: Yes, listen to that. Oh that's the first time I've ever heard an echo that long. Is anybody coming in through Skype or coming in through some sort of Internet-based thing because that could introduce that much

delay. If you are - oh Eric, yes, it might be you. If there's a way to mute one side of that that would be great.

Well anyway okay I'll try and get the audio - it does sound better now.

Okay I'm going to do the usual thing - will do threats for summary like this and we'll start dragging things into it. So I think what happened in this particular group was that they started with - is there anybody else that was in the on-phone group during Singapore that is on this call that could take us through this are we going to count on Mikey's lame summary talents again?

Okay it's Mikey's lame summary. This one I understand. This is the infrastructure. So we'll put the infrastructure one up there. That's clearly part of a taxonomy. And there are a whole series of attacks. Put those in attacks like that (unintelligible).

Cheryl Langdon-Orr: Mikey, could you just speak up a little bit?

Mikey O'Connor: Yes, I'm sorry, I'm mumbling again. Thanks Cheryl.

Cheryl Langdon-Orr: Thank you.

Mikey O'Connor: Disasters was a theme - put that in its own kind of group. I'm not sure what that group is yet. Can somebody help me out with an IDN - what is an IDN attack? Is that just another in the attack group for now or is it a different kind?

Cheryl Langdon-Orr: I know what IDN is but I'm not sure why any sort of denial of service or other sort of attack would be different between one script and another.

Mikey O'Connor: Well at this point I'm just interested in kind of getting them into clumps. And then what we can do is sort of - I think each of these is going to have to get a bit of a definition. I just want to make sure that it's not a completely different kind of thing. The border DNS...

Edmon Chung: This is Edmon. I think I heard IDN tag is - was that the question? I can probably share a little bit more.

Mikey O'Connor: ...kind of an attack that was, Edmon.

Cheryl Langdon-Orr: Yes.

Edmon Chung: Sorry, I'm in a very noisy area. But well IDN tag is really just the language tag for an IDN registration usually. And, you know, so if it's identified as Chinese or Japanese then in the registration process you would assign a tag to the IDN. That's what IDN tag is.

But I'm sorry I joined a little bit late probably. I didn't know what the context of that that was brought up.

Mikey O'Connor: Oh okay.

Cheryl Langdon-Orr: Edmon, appreciate - if I may just follow up to that, Edmon. Appreciate you're in a noisy area but actually it was an IDN attack, A-T so not a tag but an attack, A-T-T-A-C-K.

Edmon Chung: Oh I see. All right so I guess that's possibly things like phishing attacks using different characters that look alike characters and those type of things.

Cheryl Langdon-Orr: Oh.

Mikey O'Connor: That makes a lot of sense to me.

Cheryl Langdon-Orr: Okay so it's exploiting certain qualities of script variability for inverted commas, standard exploitation techniques.

Edmon Chung: I would guess that what it's talking about, yes.

Cheryl Langdon-Orr: Okay so and that was an Edmon and Cheryl duet.

Mikey O'Connor: And a very nice one it was too. I'm typing the results of that. Okay anybody want to take a crack at what needs to border DNS might have meant? Same vein. I'm not sure what that would be. So then another is sort of vulnerabilities.

Cheryl Langdon-Orr: I think that's more geek requirement...

((Crosstalk))

Cheryl Langdon-Orr: ...info than I can offer.

Mikey O'Connor: I don't know that one. I think a few of these what we'll do is we'll put - in an action item for clarification.

Cheryl Langdon-Orr: Olivier, you're a geek.

Mikey O'Connor: Didn't even get a rise out of Olivier.

Olivier Crépin-Leblond: Yes I am indeed. Olivier speaking. I am indeed but I'm also baffled by DNS border. I'm currently trying to think of this. I can imagine border gateway protocol and routing of packets but nothing to do with the DNS as such. So I'm currently scouring the Net to try and make sense of it. Thanks.

((Crosstalk))

Cheryl Langdon-Orr: So we can note that the geeks are working on it and will get back to us.

Mikey O'Connor: Yes, well and we'll put a little action item for Mark to clarify those for us rather than getting - otherwise what we could do is we could just be guys and we could invent things. That's probably not a good idea.

Cheryl Langdon-Orr: Sorry, I sound like I'm having far too much fun for a workgroup call.

Mikey O'Connor: Yes, you are...

Cheryl Langdon-Orr: I'll settle down.

Mikey O'Connor: That's what happens when people are on late at night, you know, they get frisky.

((Crosstalk))

Mikey O'Connor: ...versus dragging through our first cup of coffee.

Cheryl Langdon-Orr: Sorry, sorry.

Eric Brunner-Williams: Sorry.

Mikey O'Connor: So I'm going to move over to Roy's pile. Oop - do this without excusing myself. And I see a theme here that physical disasters and natural disasters and acts of war and terror are sort of all go into - I don't know what to call that; something like external events maybe? Call it that for now...

Cheryl Langdon-Orr: Non-Internet protocol events?

Mikey O'Connor: Oh.

Cheryl Langdon-Orr: Non-IP events?

Mikey O'Connor: Like that? Okay bugs - bugs that seems like it goes in vulnerabilities. That seems like it goes in service tags. Spam, I don't exactly know where to put that. Was anybody - Roy, are you on the call? Oh Eric's got his hand up. Sorry, I've got too many visual stimuli. Go ahead, Eric.

Eric Brunner-Williams: Yes, I was wondering if that was the case busy driving around in the middle of the screen and all...

((Crosstalk))

Mikey O'Connor: Yes, well I've got three screens going at once and I...

Eric Brunner-Williams: ...the border stuff might be and sort on the making it up category there's the synthetic rewrite modification of content in flight activity that's documented in several papers which is a threat against the integrity of the DNS created by - well presently created by monetizing ISPs and other parties which are basically intercepting on end user resolution events to generate monetized returns. So that's a - something which takes place at the border of ISP.

Mikey O'Connor: Oh so this - so this is the one up here that you're thinking is that what...

Eric Brunner-Williams: Yes, under the guise of making things up category that's my toss of the dart.

Mikey O'Connor: Good job. So is one of the things that you put in the chat...

Eric Brunner-Williams: Yes. The (EFF) paper, the (Jiang) paper, there's another paper. I've got half a dozen of them on my machine but it's 6:00 am here. I'm lucky I can find my coffee cup.

Cheryl Langdon-Orr: I was going to say hopefully with coffee at hand, yes.

Mikey O'Connor: But I'll steal your chat thing and stick it underneath the...

Eric Brunner-Williams: Fine.

Mikey O'Connor: That way we've captured that at least...

Cheryl Langdon-Orr: Patrick has his hand up, Mikey, just thought I'd help you from the bleachers here.

Mikey O'Connor: Thank you. Patrick, go ahead.

Patrick Jones: So I put my comment in chat. But I think - I know you're trying to move things around for natural categories but it might be useful if you try to keep the distinction between things that are leveraging the DNS versus things like threats against the infrastructure itself.

That's just my observation. It would be good to have discussion from others on the call if that's a good distinction between categories.

Mikey O'Connor: Give them to me again and we'll capture them at a minimum.

Patrick Jones: Well they're already up there.

((Crosstalk))

Mikey O'Connor: So go ahead.

Patrick Jones: So one heading is threats that leverage the DNS and the other is threats against the underlying infrastructure. That's one way to view it; it's not the only way and it would be good if others on the call had opinions one way or the other.

Mikey O'Connor: And one of the things to remember is that we can have multiple views of this. So it's fine to have several different ways to slice this and that's why I'm so enthusiastic about capturing these because we may indeed find that there are a whole bunch of different ways to slice this stuff. Okay so maybe I'm going to make a (thing) on that. Like that.

Let's see, hands up - Eric, is that an old hand or a new hand?

Eric Brunner-Williams: It's my other hand.

Mikey O'Connor: It's your other hand, go ahead.

Eric Brunner-Williams: Yes I think I understand what Patrick is - or I understand something from what Patrick said which is there is a meaningful difference between walking into a facility and pulling the plug; that is a physical attack on the service offered by the facility, and things which are achievable through exploiting the DNS.

Allow me though to suggest that there is something in between those which just makes life more wonderful and confusing. So I'm - so take the example of the (Egyptian) withdrawal of prefixes.

Had the withdrawal of prefixes been followed immediately by a re-announcement of the prefixes and then followed immediately by a withdrawal announcement and then back with another availability route flap would have been created. And this route flap could have propagated into the default-free zone.

And so all the routers in creation could be busy trying to recalculate what the global reachability table looks like and be unable to actually forward packets. So DNS service would fail at some arbitrary location on the surface of the earth because someone in Egypt was flipping the lights on and off very rapidly.

So that's where we have a physical effect that appears to be (local) and in scope but actually due to the - then effect a latent defect or effect on BGP4 actually that becomes a protocol attack and the attack

vector is global in nature since it reaches default-free zone. Thank you very much.

Mikey O'Connor: Would you - so I think what I heard you driving towards, Eric, is that in addition to the two that Patrick put in that taxonomy there's maybe one more in between those two?

Eric Brunner-Williams: Yes, that you can turn on the lights in someplace and actually turn off the lights someplace else because of that; action at a distance.

Mikey O'Connor: So could that be considered part of the threats that leverage the DNS?

Eric Brunner-Williams: No I think that's actually an attack on the protocol layer below the DNS.

Mikey O'Connor: That's what I was going for. Protocol - whoop.

Eric Brunner-Williams: The DNS is something above transport so this is actually an attack on the routing layer or on, you know, the ability to via TCP push tables around and recalculate them - push table up (surround) and then calculate the IP table. So whether you call it a attack on Layer 4 or Layer 3 is really a matter of taste but it's not...

((Crosstalk))

Mikey O'Connor: So if we said that the underlying infrastructure is sort of Layer 1 kind of stuff...

Eric Brunner-Williams: Then you'll confuse everyone.

Mikey O'Connor: Yes.

Eric Brunner-Williams: Layer 1 means wires.

Mikey O'Connor: Yes, physical things. I guess what I'm thinking is maybe there's - that what we're getting at here is sort of a taxonomy based on a stack in which case there would also be a layer above this.

Eric Brunner-Williams: Well it really isn't necessarily because of layers so much it's because there is the possibility of triggering what's called route flap within BGP4. So...

Mikey O'Connor: Yes that's...

Eric Brunner-Williams: ...it's another feature of BGP.

Mikey O'Connor: Yes. Yes, I get that. I was just wondering if in this taxonomy we would want in addition to the...

Eric Brunner-Williams: Well the problem with the (taxa) by layers is it just overlooks the - an alternate (taxa) if you will which is that this is a race condition in a protocol.

Mikey O'Connor: Yes.

Eric Brunner-Williams: So...

Mikey O'Connor: Okay.

Eric Brunner-Williams: It overlooks the temporal nature of the attack and substitutes for the actual vector of attack was the temporal property of the protocol by the layer-ous notion of what the protocol is in a stack which is actually unrelated to the actual bug or exploit.

So if you were to create a taxonomy that dealt with this it would be a temporal taxonomy. It doesn't matter if you turn the lights on and then off slowly with lots of time in between them; it matters if you turn the lights on and off rapidly.

Mikey O'Connor: So we've got...

Eric Brunner-Williams: So it's not about turning on and off the lights it's about how frequently state change occurs and stage change is propagated across a bunch of (stateful) devices.

Mikey O'Connor: Got it.

Eric Brunner-Williams: And with that I'll shut up.

Mikey O'Connor: No you're doing fine. You're doing fine, Eric, just fine. But what if I did it like this, what if I put yours - so there's a layer kind of set of taxonomies, maybe - maybe not. And then there are temporal kinds of taxonomies. How about that as a way to capture your point?

I'm getting a nibble from somebody. I'm going to give Olivier the floor. Olivier, go ahead.

Olivier Crépin-Leblond: Thank you, Mikey. Olivier for the transcript record. I was just going to add onto the needs to border DNS part. I've read a little bit

and seen that border DNS servers are DNS servers that do carry the same information as the hierarchy.

So it effectively means that although you might have a single route - single routes, sorry, you might have a single routes it will not actually give you answers back shared with the rest of the network. So they will serve perhaps a local area network, they will serve a sub network.

And it actually works as a network that is...

Mikey O'Connor: You know, I think we have somebody asleep.

((Crosstalk))

Eric Brunner-Williams: Yes, it's Cheryl's husband; don't worry about it.

Olivier Crépin-Leblond: It's Cheryl's husband, no worries.

Eric Brunner-Williams: Okay so the view is what Olivier is pointing out.

Olivier Crépin-Leblond: So, yes, split DNS effectively I think. And what you have is the concept of a single DNS being endangered by the idea of having the DNS servers that do not provide the same answer as others and that are there to gear towards a specific network.

This is often found in networks which are firewalled from the outside world. And I have read a couple of papers just now, Internet drafts in IETF which originate from China.

Mikey O'Connor: So could we compress that thought into something short enough for Mikey to type? And I'm assuming, Olivier, that that's going up into this border DNS category/

Olivier Crépin-Leblond: I believe so, yes. Not - no single authoritative DNS or something to that extent or lack of DNS response integrity or something which effectively endangers the integrity of the DNS itself. Because what you're looking at is - if you're going to ask two different servers you should get the same answer but you don't.

Mikey O'Connor: Okay. So does that little thingy that I just typed sort of capture your thought well enough that we can get back to...

Olivier Crépin-Leblond: Yes, yes, that sounds good. I think it's one idea. Thank you.

Mikey O'Connor: Yes, and so then if we did that with Eric's and your clarification can we pull this down into our summary somehow? Where would it go?

Olivier Crépin-Leblond: I'm wondering whether it would go - and it's Olivier again - I'm wondering whether it would go under possible hierarchies?

Mikey O'Connor: Put it sort of down on that - as a peer with these other two like that. Does that work? We'll do it for now. Okay. Eric, go ahead.

Eric Brunner-Williams: Thank you. I want to suggest that there is utility in making a distinction between split DNS which is routinely done at organizational levels within operational network contexts and the existence of other route server constellations than the ones which are associated with the IANA route. These are very different notions of intentional inconsistency. Thank you.

Mikey O'Connor: Being a kind of screen focused kind of guy where - what would you say to summarize it and where would you put it in this sort of emerging pile of threats, Eric?

Eric Brunner-Williams: Well we've split DNSs - something that can be attacked - and administrative correctness which may be described as inconsistency from a variety of viewpoints not characterized as the same thing. So if I can piggy back on Olivier's comment a split DNS is one thing; what China does because the IANA route is broken is another.

Mikey O'Connor: Okay so this half is the split DNS half right?

Eric Brunner-Williams: Is that the one that you're currently at, the no single authoritative DNS?

Mikey O'Connor: Yes.

Eric Brunner-Williams: No I think that's a reference to there being an alternate - (free) server (constellation) within China.

Mikey O'Connor: Oh okay so maybe...

Eric Brunner-Williams: I don't think anybody's rights, (e.d.) notes that condemn Xerox operating its own internal DNS using RFT 1918 address space, that's the address as to which names map which is what the split provides.

Mikey O'Connor: Yes, okay. You said...

((Crosstalk))

Eric Brunner-Williams: To be abstract one is about addresses which are private, that is 1918 addresses; the other is about addresses which are globally routed.

Mikey O'Connor: Right.

Eric Brunner-Williams: So are the - are the names spaces associated with these underlying address resources globally unique or are they locally unique knowing that the addresses are either globally unique or locally unique.

Mikey O'Connor: Yes, Eric, the only trouble I'm having is trying to summarize...

((Crosstalk))

Eric Brunner-Williams: And to Patrick I really wouldn't try to say that this is an alternate route versus global route. From the perspective of China it's of equal value. And we are not doing ourselves a favor by deciding in advance that they're wrong. That hasn't really worked very well.

Mikey O'Connor: I'm just trying to capture - I'm going to just slap the thing that Patrick typed into the chat so that we capture it. Clearly we're going to have a long conversation about that but let's try and get back to kind of pulling these together for now rather than doing new ones.

Olivier, go ahead.

Olivier Crépin-Leblond: Thank you, Mikey. Olivier for the record. Yes, I think there is a distinction to be made between the alternate routes and the alternate answers that one gets from locally - local area networks.

But I think that what might have been meant by border DNS was to do with any possible extensions of carrier grade (unintelligible) which might require then an alternate DNS in something wider than a local area network or a private network or using private address space so that might be it.

Then again I think we might be just diverging and going a little bit too deep there if we're going to look at a top level diagram. And maybe that will be one specific subject which as you said we will spend plenty of time on. Thank you.

Mikey O'Connor: Yes, I think that's right. Actually I just noticed that we're halfway through the call so what I'm going to do is transition us - I didn't expect to summarize this in one call; never mind cover the additions to it. And so expect to see this one again next time.

But what I want to do is circle us back to the criteria discussion that we started last week. And I think that what we're going to find is that as we do both of these conversations they sort of inform each other. And so let me change windows on you. Let me save this first so that I don't (unintelligible).

Here's the criteria one that we started working on last week. A bit of an eye chart again. If people are having a hard time seeing let me know otherwise I'll just stay completely zoomed out like this for the moment.

And if it's too hard to read and you want a copy to read on your own I always publish these at the end of the calls to the wiki. And so out on the wiki page there's a page for these - for each of these topics; the threats, criteria and handling confidential information. And so if you want a copy of this just to open on your machine there's a copy out on the wiki to do that.

What we found in the call last week is that we had started to come up with a - the beginnings of a taxonomy which we had a number of criteria that had to do with security, clearly a large number of them that had to do with stability.

We had the issue of these things probably change depending on your point of view. And then we had some leftovers that we just didn't have time to get into our consolidated pile. And so what I want to do is finish this and then sort of call it a day on this one because I think what we're going to find is that after we've consolidated them then there's plenty of material for a discussion but I really just want to finish the consolidation of this one today.

And again this was the work of one of the groups. I've now kind of lost track of which group it is. But if we could find homes for these they're all sort of infrastructure type items. Again we're in criteria mode not threat mode now. Where would we - where would we want to put this? Would this be - sort of reading the whole thing as I speak.

Jörg, go ahead. Oh you may be muted, Jörg. You on mute?

Jörg Schweiger: Okay, yes, this is Jörg Schweiger for the record.

Mikey O'Connor: There you go.

Jörg Schweiger: I think you can summarize them under something like sufficient provisioning of infrastructure building blocks.

Mikey O'Connor: So just re-title this?

Jörg Schweiger: Something like, yes, sufficient provisioning of infrastructure building blocks.

Mikey O'Connor: And then put it in where? System integrity? We've got an infrastructure tag in there; maybe we just add that. Yes...

Jörg Schweiger: But I doubt that it's got to do something with integrity. Maybe it's just a criteria one level up standing for itself.

Mikey O'Connor: Okay so up here like that? Okay good deal. We're really close on this one. We have one more, timely response, which seems like it lives in the process integrity. Or well, you know, that one could live in both because we've got sort of a response time component to security. Any thoughts on that? Jörg, is that an old hand or a new one? You're muted again if it's a new one. Oh hand went away, okay.

Well for now put it at a minimum in process integrity. It could even go in incident response I suppose. Okay, Scott - is Scott on the call? I wanted to hear from Scott on a few of these he had.

Okay I'm going to call the Criteria 1 summarized with the exception of those dangling participles because I know Mark isn't on the call either.

And wanted to pause for a moment and see how you as a group would like to proceed next?

One option that occurs to me is that we could - now that we've smashed all the charts that we drew together we could start discussing each part of this. But another approach would be to have somebody kind of go off and do a sanity check edit on this first; not me but somebody if people felt like that was useful. So I sort of wanted to see how people wanted to tackle this from here.

Somebody's got their phone unmuted and they're making of a clinking maybe glassware kind of sound - pretty intriguing.

Any thoughts on how to proceed? If I don't hear anything I think what we'll go ahead and do is start going through this piece by piece as a group at least for a while to see where we get. But I was curious if people wanted to do an edit on it first. I'm not hearing...

Eric Brunner-Williams: Mikey, this is Eric. I actually don't know what this refers to at this point in time.

Mikey O'Connor: Well this...

Eric Brunner-Williams: Are we still talking about threats are we talking about some other...

Mikey O'Connor: No we're talking about...

Eric Brunner-Williams: ...thing that got mashed together?

Mikey O'Connor: We're talking about what's on the screen which is a similar diagram to the threat diagram but it's a diagram of the results of Singapore, the conversation about criteria to determine the current state of security and stability of the DNS.

Let's go ahead and just take a few minutes on a small one a little bit. All we did with this security area was combine the titles. And I think now it's not a bad idea to start refining this and discussing it to see if there are things that need to be added to this list of criteria for the security of the DNS, if these need to go into some sort of a taxonomy, if we can expand some of them, things like that.

And if we get stuck, you know, if the conversation sort of continues to be sort of silent like this I'm also willing to sort of set criteria aside for a while because clearly the threats discussion is going to occupy us for several meetings at least and maybe that's the place to focus our attention.

So, you know, I'll take a quick sense of the group on that. Would people rather just switch back to threats at this point and keep working on that? Let's do that for now and the - the ops kids can sort of take a look at these and see what we want to do next.

If we go back to the threats diagram, which is where we started the call, and we continue onto Roy's list, which is this list over here, if we took spam as a threat to the DNS what would that mean and where would it go in this sort of emerging taxonomy that we've got? Anybody want to sort of expand on that? I was sort of trying to figure out what that meant as a threat to the DNS.

Jörg, go ahead. Jörg, you may be muted, sorry about that.

Jörg Schweiger: No.

Mikey O'Connor: There you go.

Jörg Schweiger: Yes, Jörg Schweiger for the record. I doubt that spam really is a threat to the DNS, that's just by 5 cents.

((Crosstalk))

Mikey O'Connor: ...I've got a guy in the queue right behind you that might have some good contribution there. John is a pretty big deal guy on spam. John, why don't you go ahead?

John Levine: I can give you some arcane theories although I tend to agree that as DNS threats go it's not really large. The - as soon as you move to IPv6 with the enormous address space and you have spammers hopping from IP address to IP address like every time you look up like - it is fairly common for mail servers to do a reverse DNS lookup on each - on the IP address of each incoming message.

If every spam message comes from a different IP address it's going to basically be doing billions of un-cachable look ups and it's going to make DNS caches melt. This is - not everybody agrees with this but in the mail community people agree this is at least plausible enough to be worth thinking about.

I don't know if that's what he had in mind. That's the main - the main threat I can think about is just that the larger IPv6 address space and

the large volume of spam messages makes it an indirect and probably not deliberate attack on the DNS.

Want me to go through that again for anybody who didn't understand what I said?

Mikey O'Connor: I kind of followed it. See what I'm typing in there and see whether this makes sense, John.

John Levine: Yes, it's both volume related and also it - the query pattern makes normal caches not work.

Mikey O'Connor: Which kind of caching, DNS caching?

John Levine: Regular DNS caching, yes. I mean, DNS caching assumes that you're going to - I mean, like any cache assumes that you're going to get repeated queries for the same thing. And since the v4 address space is like - it's comparatively small you tend to get multiple mail messages from the same host so the cache does what it's supposed to.

Mikey O'Connor: This is clearly colloquial note taking but...

John Levine: Yes.

Mikey O'Connor: It can easily be - well, you know, that's a plausible theory; it's one we could certainly argue about. Where would it go over here in the - in this hierarchy? We've got a...

John Levine: I'd say it's your - it's...

Mikey O'Connor: It's not really an attack it's really kind of almost unintentional...

John Levine: It's somewhere between an attack and a vulnerability.

Mikey O'Connor: Yes - that.

John Levine: Yes, I mean, the presumption is the spammers would be unlikely to do this with their goal being to wreck the DNS although it's possible that - that's sort of an intermediate stage on the way to defeating the DNS-based anti-spam techniques that people use.

Mikey O'Connor: So maybe it is a vulnerability more than an attack...

John Levine: Yes.

Mikey O'Connor: ...for the most part. You know, if we put, you know, attacks is things that people do on purpose and vulnerabilities - well no, not really. You're right. Leave it.

John Levine: Yes, I mean, they're doing it on purpose but then well, you know, it's like...

Mikey O'Connor: Yes, they may not be.

John Levine: Yes I think this - I think what we just demonstrated it's in real life every taxonomy no matter how beautiful has things that don't quite fit.

Mikey O'Connor: Yes it has fuzzy things that don't fit. And the main thing - I really don't want to lose things just because they don't fit in a taxonomy especially this early in developing it. So we'll leave it up there.

Thanks, John. Olivier, go ahead.

Olivier Crépin-Leblond: Thank you, Mikey. I was just going to mention for the record that there actually is currently a religious war going on in one of the discussion lists specific to IPv6 with regards to having SMTP mailers needing a valid reverse IP address. Some don't think that it's needed; some thing it is. Some think that it has fallen behind the times and people don't bother. And some others think that the DNS is so broken already that many operators don't bother.

So it might be yet again another huge subject for a discussion. Thanks very much.

Mikey O'Connor: So is that broader than just spam? And so as a result rather than putting spam as the heading the heading under which this sits is a broader thing?

Olivier Crépin-Leblond: It's related to email specifically. I would say spam specifically but email. And yes spammers do make use of this and some anti-spam systems make use of checking for the reverse DNS, reverse IP. And if it doesn't have one then it will not accept the email.

But with IPv6 coming up and things not being set up properly it might well be that a lot of general mail gets rejected by this. But yet again maybe we're not going to go deep into the subject but list it here. Thanks.

Mikey O'Connor: Yes, this is clearly one that we - we'll be able to take a much deeper dive on when we come back to it. So for now I think we'll capture it this

way. And hopefully there's enough notes there that will remind us of this discussion. If there isn't let me know because I could add something about - something along the lines of...

Olivier Crépin-Leblond: Reverse DNS. Olivier for the record.

Mikey O'Connor: Reverse DNS in SMTP servers; is that primarily where that goes?

Olivier Crépin-Leblond: Reverse DNS for SMTP servers. Thanks.

Mikey O'Connor: All these issues. Just as enough of a reminder. Luis, go ahead.

Luis Diego-Espinoza: Yes, just I thought this kind of attack could be a kind of indirect attack like Conficker or the hacker or spammers have a different target. But in the way they use DNS. That's my thought.

Mikey O'Connor: So would you - well there's direct attack...

Luis Diego-Espinoza: Some kind of attack but indirect.

Mikey O'Connor: Maybe put this under there like that? I kind of like the distinction between direct and indirect attacks. Let's capture that for future thinking. Thanks, Luis, that's great.

Let's move onto - no let's not move on. It's three minute to the top of the hour. This is a very good place to stop, sorry about that; I lost track of time. I think we'll pause here and just pick it up in the exact same spot on our next call.

Clearly we've got plenty of material to get through and then once we get through just consolidating it we are going to have lots of conversation clarifying and refining this. But I want to take a moment and make sure that this process feels okay to people.

I think we're doing great. And just want to make sure that I am not delusional because I think that this is going to feel a bit slow for a while until we get some themes emerging. And I think we're doing a terrific job. So getting a few little thumbs up out there in participant-land so good we'll keep doing this.

And I'll publish this - the current state of affairs so that you can look at it. And maybe it would be good for all of us to sort of take a look at this and start to think about possible taxonomies that we're not capturing yet. I mean, maybe this is - I do want to get this into some taxonomies otherwise it becomes completely unwieldy. But I think we're off to a great start.

So with that it's the top of the hour. I thank you all and I'll see you in a week.

Cheryl Langdon-Orr: Thanks Mikey.

Edmon Chung: Bye.

Mikey O'Connor: Glen, I think we can stop the recording. Do stuff like that if you're still on the call. Who's the operator on the call today?

Coordinator: Hi, (Ricardo) here.

Glen de Saint Géry: Mikey, can you here me?

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

Glen de Saint Géry: I was on mute, sorry.

Mikey O'Connor: There you go.

Glen de Saint Géry: Yes, (Ricardo), can you hear us?

Coordinator: Yes absolutely.

Glen de Saint Géry: Thank you. Can you stop the recording please? And thank you very much for taking such good care of the call.

Coordinator: Not problem. My pleasure.

Glen de Saint Géry: Thank you.

Mikey O'Connor: Great job to both of you.

Glen de Saint Géry: Thank you Mikey.

Mikey O'Connor: Thanks a million, Glen, for all your help. It went...

END