Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
01 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 01 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-20110901-en.mp3

On page:

http://gnso.icann.org/calendar/#sep
(transcripts and recordings are found on the calendar page) **Attendees on the call: At Large Members**

- Cheryl Langdon-Orr
- John Levine

ccNSO Members

- Jörg Schweiger, .de (co-chair)
- Takayasu Matsuura, .jp
- Katrina Sataki, .lv
- Wim Degezelle, CENTR
- Jaques Latour, .ca
- Luis Diego Espinoza,.cr
- Ondrej Filip, .cz

GNSO Members

- Greg Aaron – (RySG)
- Scott McCormick – (CBUC)
- Mikey O'Connor – (CBUC) (co-chair)
- Rafik Dammak – (NCSG)
- Keith Drazek – (RySG)

NRO Memberers

- Carlos Martinez (LACNIC)
- Arturo Servin (LACNIC)

SSAC

- Jim Galvin (SSAC)

ICANN Staff:

Bart Boswinkel

Julie Hedlund
Patrick Jones
Glen de Saint Géry

Apologies:
Olivier Crepin-Leblond
Sean Copeland, .vi

Mark Kosters (SSAC) Don Blumenthal – (RySG) David Conrad (SSAC)

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

Gisella Gruber-White: Thank you. Good morning, good afternoon to everyone on today's BSFA call on Thursday, the first of September.

We have Cheryl Langdon-Orr, Mike O'Connor, Jacques Latour, Katrina Sataki, Luis Diego Espinoza, Scott McCormick, (Takaya Samatsura), Keith Drazek, Joerg Schweiger, Wim Degezelle, Andres Phillip, Arturo Servin, Jim Galvin, Greg Aaron. From staff we have Julie Hedlund, Patrick Jones, Glen de Saint Gery, Bart Boswinnkeland myself Gisella Gruber.

Apologies today noted from Olivier Crepin-LeBlond, Sean Copeland, Don Blumenthal. If I could also please remind everyone to state their names when speaking for transcript purposes. Also we were not able to join Rafik Dammak nor Mohamed El Bashir on this call. Their phones weren't answering. Thank you. Over to you Mikey.

Mikey O'Connor: Thanks Gisella and welcome all. We're going to do pretty much the same agenda as last time, mostly working on our threats document, which is on the screen in front of you.

And I've posted just recently about a half an hour ago, I posted the same mind map that you see on the screen to the wiki page. And the link is there, it's the last one on the bottom of the page. And I posted it just in the format that has the viewer so you can expand and navigate the mind map. It's now gotten quite bushy.

So it's going to be a lot of driving around on the screen and it may be easier to follow along if you want with your own copy. So first order of business is does anybody have an update to their statement of interests that they want to share with the group?

Okay. Here is sort of where things stand. I at the tail end of the last call asked the group whether they wanted to continue the build the map on the screen exercise that we've been doing for the last couple of weeks or let Mikey go ahead and take a stab at it on his own.

And the sense of the group I got was why don't you go ahead and do that. So I did a couple of things this week and I want to start this off by saying that I have absolutely no editorial pride at all so if there is anything wrong blame Mikey and we'll fix it. But what I did was I went through first a couple of SAC reports, SAC 40 and 44, and I stitched those in.

Then I read all of the SAC reports that are on their page and found that some of them were relevant to what we're doing or at least appeared that way to me. So I stitched them in in various places and again the thing you'll - no editorial pride if I got that wrong or if you disagree. That's fine. That's really still in my mind a very early draft at this.

And then what I did is I went through and I reorganized the threats to compress out some of the redundancy and so on. And so I forced it into a hierarchy, which you may or may not agree with and again we have lots of choices there.

So there are a bunch of ways to look at this that may not be right and I think what we need to do is continue through this today just to give you a sense of where we're at with several questions in mind.

One is are there any missing still? I still view us in the stage of really trying to bring things in, not get rid of things yet. We've got plenty of time to do that. So if there are some that are on your mind that you don't see here, I'm really interested in those, either on the call or via email on the list or whatever. Another thing that I'm interested in is other sources of information.

So for example, Patrick Jones pointed me at a document that came out in 2007 or '08 that was about registry fail over on the ops call. And so I went ahead and read that and stitched that in. It was a terrific document. There was a bunch of really good stuff in there. And all credit to Patrick. He wrote it. So if you as individuals have written stuff don't be shy about pointing it out to the rest of us because there is still lots I think.

One of the thing that we talked good about on the ops call is sort of what is our objective and when is it due. And our objective is to get a really well defined list of threats by Dakar. So we're making fine progress toward that goal and you know, if you backed us up against a wall and said that we had to produce something tomorrow I think we could produce a pretty good slide deck for a meeting tomorrow based on what we've got already.

But we have lots of time to make it better. So let me take you through that. Feel free to jump in but let me just give you a sense of what's underneath this. There is quite a bit underneath each layer so I'm going to sort of take it section by section. And so you can see that just in that first threats to underlying infrastructure part we have from a variety of places a lot of information that we can read and think about.

You know, there were - this goes on and on and I'm not going to take you through all of this. But you know, there is indeed quite a substantial amount of

information underneath this. And that's why I've started saving the mind map on the Web page with a viewer so that you can do what I'm doing right now and sort of expand and then collapse little branches on this tree.

And so as we go through this what starts to emerge at least for me is that we have the sort of infrastructure threats which may or may not be attacks. They may just be like storms and so on. And in fact, there was an interesting point on Circle IT about the effect of the hurricane here in the US last week. Luis, go ahead.

Luis Diego Espinoza: Yes. Thank you Mikey. Luis Espinoza from Costa Rica. I think it's a good thing to try to cover all the popular threats but known threats. But my question is in this team if a new threat emerged, is it possible to put in there? I it possible to 7cover new threats that maybe we don't know now? That's my question.

Mikey O'Connor: Yes. That's a great question and I think that what - we as a chartered body have a limited life. We have a beginning and a middle and an end. And it seems to me that we can certainly cover any threats that emerge while we are still going.

At least from my vantage point as the scribe, it's very easy to insert new information into this document right now. And it may be that at some point we'll want to draw a line and say all right, the door for new threats is closed. But that I think is fairly late in the process. It's certainly not before Dakar and it may not even have to be before the end of the next phase, which is where we actually analyze these threats.

But I think that probably towards the very end of the work we'll have to essentially say that's enough. We're going to stop analyzing new threats now and I think it's a good idea to add that to the list of things to do and put that on the work plan so that we all kind of know when we're closing the door to new threats. So I'll take an (action item) to do that.

Good point. Anything else on what you've seen so far before I move on? All right. Let's shrink this one. The next list is still a little bit rugged I think. It turns out there is quite a lot of information underneath this. I didn't really get through this quite as deeply as I wanted to but I think that there may be another layer of hierarchy here that we can put this into.

And one of the interesting - well, several interesting questions have sort of emerged as I have been looking at this. One is who is being attacked needs to be understood. In some cases it's everybody, in other cases it's not. And I think we should put this into those (piles). Another thing that is emerging in my mind is that some of these attacks are not unique to people who operate in DNS infrastructure or the DNS.

Some of these things are just essentially for example, gaining control of a password is an attack that's not unique to our world. It's something that anybody who operates a public facing (authenticated) site on the net needs to deal with. And so what we may want to start thinking about is segregating our work into issues, which are essentially addressed by standard security practices and those that aren't.

Because to the extent that some of these things can be handled by routine security or operational planning rather than reinventing a lot of information about that, I think what we might want to do is just say these are things that ought to be addressed by normal security practice so that we can focus on the things that are really unique to the DNS issue.

So that's something for you to ponder as we go through this. Anyway, so there is a lot of information under here. You know, you look at DDOS just as an example, there is plenty of detail to read about. Packet interception not so much but you get down into this one, the gain control of passwords and there is so much information it just explodes.

And so one of the things that we need to start thinking about is well, what do we do next with all of this. And one option is to start breaking into groups at some point certainly when we do the analysis. I think this is going to be a good foundation for a group that's working on any given issue, which is why I'm not feeling at all bad about this being a very large document right now.

Because I think that this gives the analysis groups sort of a head start on their work. But it does make it a little unwieldy unless you use this sort of mind mapping approach to it. But I think that especially direct attacks and indirect attacks is a place for you to go look and start thinking about ones that we missed or documents that you are aware of that paint a discussion of this.

For example, on the last call I forgot who, sorry - Roy, somebody - pointed me at an RFC and I ran off and read it and it shows up actually in a lot of places. But you can see that another thing that I started to do is give us hints as to where the information came from so that we can get back to it. And then what I usually did if I had time, you know, this isn't the main one.

I can't remember where the main discussion of 3833 is. But somewhere in here I've actually summarized the document so that we've got a start on that. Again, this is mostly for the folks who analyze these as we move forward. So I think one thing I want to sort of highlight is we've got choices on what the hierarchy is.

This direct/indirect threats to underlying infrastructure is fine. But if it's not fine for you, that's okay with me. Let's circle back to this. But let me continue the tour. We have a very similar hierarchy in the vulnerabilities one and it looks so innocent - operational issues, this tiny little section. But when you expand it, it gets pretty big.

So I'll give you this one. You can see that there is a lot of information. Oops - about business and process vulnerabilities and a whole bunch of documents that I've found it's pointed to. Again, I'm not too worried about this being really

busy because I think it's good material for people when we get to analyzing it. The same sort of thing with infrastructure vulnerabilities.

A whole bunch of that's where our single point of failure stuff wound up, that's where registry failure kinds of things wound up and so on. And so unlike task calls where I was really just using this for recording this, I think it's time for you all to dig in to the version of this that is out on the Web site because this will take some time for you to digest.

That's good. Anyway. So there are a bunch of operational issues. There was interestingly as I went through this, there was quite a lot of information that I decided really went into a kind of managerial bucket rather than an operational failure. It is sort of splitting hairs, a pretty subtle distinction and I could be talked out of this.

But there does seem to be quite a lot of managerial stuff that we could highlight in our discussion. Then there is a whole series of sort of underlying infrastructure kinds of things. And then I had one left over I just didn't know what to do with. I think as time goes by this will find a home somewhere. But I left it up on the top level for now.

So again, that's sort of where things are at. It's now so big that it's going to be hard actually revise this on this call with so many people on the call. But I wanted to give you at least an introduction to where it is now. Again, I really strongly encourage you to go out and take a look at the document that's on the wiki. While I don't think we're done, I think we are beginning to see the light at the end of the tunnel on getting at least the basic list out there.

So we start to pitch into the sort of next steps on our work plan, which among other things is to get this list into enough shape that we can start taking this out to other people, other security experts who aren't directly involved with this working group but might also have ideas about things to add.

So I'm going to stop with the tour right now and just give you all a chance to speak up and say you know, is this good, is this bad, is it too hard, too big, too weird, whatever.

Jacques Latour: Mikey, Jacques.

Mikey O'Connor: Go ahead Jacques.

Jacques Latour: I'm just - a lot of this stuff we have in here is somehow maps to like another's ISO 27,000 standards. It's - I don't know if you ever saw that but it's like a framework for doing security management.

Mikey O'Connor: Yes.

Jacques Latour: And a lot of what we've covered falls under various portions of that framework to do security management.

Mikey O'Connor: Yes, I agree. And I think that there is an opportunity there to go through these and identify which ones do and essentially make a choice.

But one choice would be to say if it falls under a pre-existing security standard like ISO 27,000 or the credit card industry one or whatever, that we essentially take those out and say that those should be addressed by that framework. That I think is a big choice for us to make. And I didn't as your scribe, I didn't want to make that choice for you.

But I think that there is an analysis to do along those lines and some leverage once we do that analysis where we could essentially point to those pre-existing security management standards and say you should do these. Is that sort of where you're going with that?

Jacques Latour: There are a lot of people spent a lot of time defining standards and they're all (poisons), right? We have to - because right now we're creating our own I

think and maybe we're aligned with one of them but I don't know which one is the best for us to use.

Mikey O'Connor: Yes. Right. I think that to the extent that we get leverage, to the extent that it helps, we should. To the extent that it does not, we shouldn't be bound to that. But I agree we should think about that and try to decide whether that helps us or not. So I'll put that on the list of questions for the future.

Joerg Schweiger: Mikey, this is Joerg Schweiger, may I interrupt you?

Mikey O'Connor: Sure. Go ahead.

Joerg Schweiger: I'm not so sure whether I should agree with the suggestion made by Jacques or not. That is due to the fact that I personally do think that ISO 27,000 is fairly abstract. And it does not give us a certain hint to my point of view what to do with the security vulnerabilities, threats and so on.

So I doubt that we could easily just leave something out for the ISO to be addressed. But more so I think that our threats or the threats we are dealing with in this working group are so specific that we do have to address them by ourselves and that we could not give them away to somebody else to address.

Mikey O'Connor: I agree with that too Joerg. I'm thinking that what I'm really reminded of as I went through this process I'm reminded of the exercise that some of us did on the high security TLD advisory group, which what we would up doing was basically replicating a lot of the information that's in some of those pre-existing standards and best practices.

And we had so much of that that we didn't ever focus on the issues that are unique to the DNS. And so I agree with you that anything that's unique to the DNS I think we have to hold on to. I think we have to keep that front and center in our analysis.

But if we can find a whole bunch of things you know, for example a lot of the if I go up into the underlying infrastructure ones, a lot of things like this you know, disk drive failures, physical site failures, applications - things like these are not unique to the DNS. They are really standards and best practices for running any major data center that has got to have high up time.

And what we might want to do is essentially go through these lists and say all right, these items can be eventually handled by saying you know in order to address these just follow the best practices in PCI or ISO 2700 or whatever.

I mean I think we'd have to choose something. But as soon as it's unique to the DNS one, I think absolutely we have to keep it in our analysis.

Anything else, any other reactions to this giant bushy tree that I've built, that we've built? Shouldn't say I, sorry about that. Let me focus you on the question about are there other sources of information that I've been doing.

Is essentially building another tree like this where I've been summarizing documents that just - and mostly so that I can then stitch them into this but I don't feel like I'm familiar enough with this landscape to know about them all. So again you know I've read all of the SSAC reports, Patrick's registry fail over document that was on the web.

Memorized that RFC, that's about it. So if those of you who deal with this sort of day to day, yeah, and Patrick is asking in the chat am I keeping a source tree and the answer is yes I am.

It's a document that's about as big as this one. Because it's not just the sources and the links but it's also the summaries. I agree, I think it's going to be a terrific appendix.

I also kept track of - there's a pretty good emerging list of acronyms and the beginnings of a glossary that I've been starting to build, I think we're going ot need that as well.

So I've been keeping track of that too. So I think that the really important question right now is what other sources either documents that are on the net or other people that we should draw into this?

But I think primarily right now we have a pretty astounding group of people in the working group and on this call. So I'm not being shy about saying can you all think of other things that we go look at and summarize this way?

And either fire them into the chat or describe them, you know jump on the call bridge here or send them to the list. And then I think the next phase of this is to start boiling it down a bit so that it's a little bit more - a little easier to manage.

Not getting overwhelmed here, yes, Patrick's saying - Patrick go ahead.

Patrick Jones: Yeah, so my suggestion and I put it in the chat but asks the same question to the whole mailing list, but when you do that attach your link to the wiki of this latest document as a reminder that you know here's what the group's done so far.

It's missing something, probably a hyperlink or pointer to documents that can then be added in.

But that we really need to start to collect any extra sources or experts that are out there.

Mikey O'Connor: That's a good idea. I'll do that. I'm just writing myself a note. And you know I can put out some versions of this that are a little easier to handle than that bondable Adobe document as well.

So that people don't have to dig into that, it's a little weird the first item you look at it. Okay, Keith is typing. Keith why don't you just speak? Everybody's being so good about talking into the chat but I get so lonely talking at you.

Keith Drazek: Thanks Mikey, yeah this is Keith. I just wanted to - I was just going to type that you know I'd like to thank Mikey for all the hard work and effort and time that you've put into you know the compiling this working document.

And what I was going to say is that I need to spend some time myself reviewing it in more detail before I think I can have any sort of meaningful comments at this point.

But I plan to do that and we'll bring some more substantive comments to the next call.

Mikey O'Connor: Yeah that's terrific, thanks Keith and thanks for the kind words. I actually quite love doing this kind of thing, it's a great way to learn about something and so I had a pretty darned good time.

I couldn't go outside and work anyway because I had whacked the heck out of my finger and so this was a terrific project to do but thanks for the good words.

And I agree, I mean I still am finding things in this document because I scream along and I paste it in, you know for example the stuff that's on the screen, that's just a cut and paste out of Patrick's document.

And a lot of times it takes me two or three times across a given set of bullets before they start to sink in. So I'm having sort of the same reaction.

I need to look at this again and start thinking about sort of my reactions to it all.

Keith Drazek: Yeah, this is Keith again. I mean I think as somebody who I guess has done a fair amount of cutting and pasting in my working career, I think that the risk is - as you do that especially in a large document that you risk having - losing a little bit of focus and your definitions start to get a little bit muddled.

So that's one of the things that I want to take a careful look at in my review is to make sure that you know that the focus of you know the work of the group is not being sort of muddled by the cutting and the pasting and that we keep clear what the definitions are and what our goals are.

But you know I think this is a great working document.

Mikey O'Connor: Absolutely and I couldn't have said it better than that. I think actually you're bringing out what is bothering me right now which is the need to stay focused on those - you know our mission is to assess the security and stability of the DNS today.

And not get distracted by things that don't directly bear on that.

Keith Drazek: Yeah, that's exactly right Mikey and I'll give you an example, on the page where we are right now, and you know it really depends on what our definitions of the DNS are, right?

One of the items under system failure is billing and collection server fails, right? That's potentially an interruption of business, it could prevent somebody from registering a new domain name or renewing an existing domain name.

But is that what we're really considering as a threat to the DNS, right? And so I think that - and I don't know the answer to that, maybe it is and - but I think that's the type of thing that we all need to go through this document as it stands today and really sort of narrow the focus of what exactly you know are

we considering DNS and what is - you know what are the things that we really ought to be focusing on as a working group.

That may be a reasonable thing to include but it may not be something that this group you know thinks should be in our purview. But I think we should all be looking at the document as it exists today in this relatively early stage to make sure that we sort of keep our focus.

Mikey O'Connor: Yeah, I think that's absolutely right. And it may be that this document has gotten so big that we'll need to break that work into chunks. You know we may want to think about splitting some of this so that not everybody has to read everything in the whole document.

So as you look at this hierarchy if there's a part of it that interests you as an individual and you want to form a sort of sub group, sub team, whatever to go take a first pass, and then come back to the rest of us with your assessment it could be as simple as just going through and sort of pick, marking one saying you know these are the ones that we think might want to move out of the focus, you know picking on that billing and collection server example.

Keith Drazek: Greg Aaron has his hand up.

Mikey O'Connor: Yeah, I know. Greg, go ahead. You may be muted Greg.

Greg Aaron: Oops.

Mikey O'Connor: There you go, now you're on.

Greg Aaron: Okay, hi it's Greg. Can you hear me?

Mikey O'Connor: Yep.

Greg Aaron: Okay. Well I think one of the things we need to do is look at our charter which does give us direction on this issue. Specifically you know it's talking about the DNS and it says that quote, "the working group should limit its activities to considering issues at the root and top level domains within the framework of ICANN's coordinating role".

And I'll send that quote and some other notes out to the mailing list, but what our charter seems to tell us is we're not to be concerned about everything on the internet.

And not everything unique to the DNS either, and some previous working groups have actually done some thinking on this which we can point our membership to.

So there are certainly some topics on this sheet that don't qualify under that charter I think, things like domain hijacking, cybersquatting, phishing and some other things clearly could be put aside so we can focus on the core issues.

Thanks.

Mikey O'Connor: Thanks Greg and I will send you your $50 after the call for leading into a topic that we need to talk about if I can get to it. I'm going to change what I'm sharing. Go to the work plan. All right.

So if I think I still have - going to grab navigation away from you because I want to - work plan, sort of highlight where our - where we're at right now is basically this page, the identify threats page.

And more specifically where we are is we're at a list developing step. We're basically at Step 2. Step 3 is the - is what we're headed towards I think which is to go out of our own membership and seek lists from others.

And so maybe we're even at Step 4 which is we have a preliminary list, but it's way too broad. And I think Greg what you're pointing us to is Step 5 which is determine which of these threats are in scope and then to the extent that we have scope issues to resolve, we resolve them.

So I think that's sort of where we're all headed. You know I could sort of bend Keith's comments into the same...

Greg Aaron: And I would note - this is Greg again, I would note that if we're going to go ask people for their ideas and suggestions about what we should look at we should also be telling them the parameters of what we're looking for.

Otherwise we may get an undifferentiated list of stuff which might not be relevant.

Mikey O'Connor: Yep. I mean one thing we might want to do is take a first pass at the scope before we go out so that we don't startle people with this giant bushy list.

That's something that I would be pretty open to. Oh my God, Firefox wants to update itself right now. I'm sorry Firefox.

So I think that what we've got is a good foundation but I do think that it's time to start going through this with a critical eye.

And identifying those things that we can start to drag out of scope for several reasons, one you know I think Luis's earlier comment is another thing that we could use to narrow the scope of this, which is to the extent that these are routine items that are handled by good security practice more broadly, we - not necessarily unique to the DNS then I think we could make that a pile.

We could take another pile and say this is a pile of stuff that's relevant to ICANN in general but it's outside the scope of our charter. And then maybe

that's the point at which we go out to other people, having done that first pass.

And so I think again what it needs is people, you should go through this document with a fairly critical eye now and start identifying those things which could be removed without harming our mission which is to go after the DNS at the root and top level domains.

Any other thoughts from folks? Those are good ones. Okay, I'm going to leave us - sort of depart from that topic at this point and swing us around very briefly to point that came up on the last call which was a question about whether we could change the timing of the call or rotate the call.

Because folks in the Asia Pacific region really - this is a very inconvenient time for them and we talked a bit about this, we talked quite a bit about this in the co-chair call on Monday.

And I hate to be the bearer of bad news but we decided that in our experience on lots of other working groups it's been very difficult to hold a group together with staggered call times.

So what we have concluded is that this isn't really a very good idea. The 8:00 am for me, 13:00 UTC time that we're on right now seems to be a sweet spot that works pretty well for people in Australia, Europe and clearly the United States.

And there really isn't another good sweet spot time like that when we go out to 23:00 UTC it gets very late for people in Europe. They're really - there is no good one.

The small piece of good news that I have to offer is that when we get further into the analytic part of this project it may make sense to split the group into

some sub groups and some of those sub groups could cluster in such a way that we could have two call times to meet the needs of sub groups.

And one of those call times could be something like that 23:00 UTC hour but at least for now after a really long discussion about this we concluded that it was just too disruptive to do that. So we're not going to do that at least until Dakar.

We talked about the possibility of doing an experiment and we concluded that the experiment was almost guaranteed to fail and we didn't want to run the group through that pain.

So I'll publish that to the list after the call. But that's sort of where that stands at the moment. I think that's it for today's call unless people have any other business that they'd like to bring up.

We're sort of at the point where you as individuals now have a pretty good document to go start thinking about and as you get into that document and you find it inconvenient, what I will do is I will publish that document in several forms on the wiki right after the call.

I will publish it as a Word document and I'll publish it as a web document. The web document is basically the whole outline and so it will be very tall as will the Word document.

But you know the mind map that I'm using is unfortunately proprietary software and very expensive and so it's not feasible I don't think for you all to use it that way.

I'm all ears in terms of how to go through this and move things into piles and I think that that's probably the focus of the next few calls is to start saying which of these things can we pull out of this hierarchy and put aside?

Not that we're going to ignore them, I think we'll list them in the report, but we'll list them as things that we feel are outside the scope of our work but not to be lost track of.

So I think that's our focus for the next few calls and if it turns out that this is something that needs to happen in sub groups I'm fine with that.

It may well be that that's the case. So that's it for me. Last call for any other agenda items?

Man: Mikey?

Mikey O'Connor: Go ahead.

Man: I think a lot of us actually have mind map so if you actually publish that actual file with the PDF then maybe we can manipulate it, play with it and see what we can do.

Mikey O'Connor: I'm using a proprietary one rather than the freeware one. I could try and export this into the freeware one. Which one...

Man: Are you using MindJet?

Mikey O'Connor: Yes, I am using MindJet.

Man: Yeah, I think a lot of people actually have MindJet.

Mikey O'Connor: Really? Throw your hands up if you've got MindJet, just go up there and click on the little thing, Jacque has done it, great way to do that and essentially what I will do is I'll post the MindJet file and then I'll also see if I can export it into - there's one called FreeMind that's an open source project.

And I'll see if I can figure out a way to export into that too. Cool. Okay, that's it for last call, last chance for me. That's it for today, thanks all and the likelihood is that the co-chair call probably won't happen next week Monday because it's a holiday, Monday's a holiday in the US and I think we'll lose a lot of people.

So we'll see you in a week and if anybody has any course corrections or ideas, don't be shy about posting them to the list. See you then. Gisella I think we can wrap it up.

END