Transcript
DNS Security and Stability Analysis Working Group (DSSA WG)
18 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 18 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-20110818-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
- Andre Thompson
- Patrick Vande Walle

ccNSO Members

- Luis Diego Espinoza, .cr
- Jörg Schweiger, .de (co-chair)
- Chris Wright, .au
- Katrina Sataki, .lv
- Wim Degezelle, CENTR
- Roy Arends, .uk
- Jaques Latour, .ca

GNSO Members

- Greg Aaron – (RySG)
- George Asare-Sakyi – (NCSG)
- Mikey O'Connor – (CBUC) (co-chair)
- Rafik Dammak, GNSO

NRO Members

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

SSAC

- Rick Wilhelm, Network Solutions

ICANN Staff: Bart Boswinkel

Patrick Jones

Julie Hedlund
Gisella Gruber-White
Glen de Saint Géry

Apologies:

Takayasu Matsuura, .jp

Adam Palmer – (CBUC)

Rossella Mattioli – (NCSG)

Chris Wright, .au
Edmon Chung

Ondrej Filip, .cz

Don Blumenthal – (RySG)

Andrew de la Haye (NRO Member) - for the next 4 weeks

Mohamed El Bashir (At-Large)

David Conrad (SSAC)

Jim Galvin (SSAC)
Mark Kosters (SSAC)

Coordinator: Please go ahead; the call is now being recorded.

Gisella Gruber-White: Thank you. Good morning, good afternoon, good evening to everyone. On today's DSSA call on Thursday the 18th of August we have Rafik Dammak, Cheryl Langdon-Orr, Mike O'Connor, Patrick Vande Walle, George

Asare Sakyi, Andre Thompson, Jacques Latour, Olivier Crépin-Leblond, Roy Arends, Arturo Servin, Jörg Schweiger, Richard Wilhelm, Wim Degezelle, Greg Aaron; from staff we have Patrick Jones, Julie Hedlund, Bart Boswinkel, Glen DeSaintgery and myself, Gisella Gruber. I hope I haven't left anyone off the list.

And apologies today from Adam Palmer, Chris Wright, Edmon Chung, Andre de la Haye, Andre Philip, Rosella Mattioli, Don Blumenthal, Mark Kosters, Mohammed El Bashir and David Conrad.

Could I please also remind everyone to state their names when speaking for transcript purposes especially when you have so many people on the call. Thank you, over to you Mikey.

Mikey O'Connor: Thanks Gisella. Thanks everybody for joining today. And we're going to just do our standard thing where we take a moment to see if anybody has a change to their statement of interest that they should let us know about that and then we'll get on with the main event.

All right I think we have - Olivier do you want to fill us in a little bit on Eric?

Olivier Crépin-Leblond: Thank you very much, Mikey. It's Olivier here. Actually you probably know more than I do because frankly you've been notified that Eric will drop off the working group...

Mikey O'Connor: Yes, okay.

Olivier Crépin-Leblond: ...I understand.

Mikey O'Connor: Let me...

Olivier Crépin-Leblond: So I don't know what the process is but I'll leave it to us to deal with this. Thank you.

Mikey O'Connor: Yes well we'll - in our ongoing tradition as co-chairs we'll invent something. Anyway I got a note from Eric Bruner-Williams that said that he's no longer a part of - he said the ALAC; I was thinking maybe At Large. But anyway he is dropping off the DSSA.

So Gisella and Glen, if you could sort of note that and do all the needful in terms of email lists and so on that would be good. And so the reason he's not on the call today is because he's dropped off the working group.

Okay...

Cheryl Langdon-Orr: This is Cheryl here, Mikey.

Mikey O'Connor: Pardon me?

Cheryl Langdon-Orr: Cheryl here, Mikey.

Mikey O'Connor: Yes, go ahead, Cheryl.

Cheryl Langdon-Orr: I think it is important to note that Eric is a individual member representative in (Arolo). And the representation he was bringing into DSSA was very much on behalf of that region. And it may be appropriate to see whether there was a alternative or another suitably technically qualified person who was put forward to the ALAC for recommendation into the DSSA on behalf of that region.

ALAC did take a five-region approach to the population of our representatives to this workgroup. And it might be worthwhile to - with the ALAC meeting coming up early next week to bounce that back to the ALAC via Olivier.

Mikey O'Connor: That sounds like a plan to me. Olivier, does that work for you too?

Olivier Crépin-Leblond: Hello, Mikey. Thank you. Olivier for the record. Yes it works with me. What I would therefore require is an email from the working group to advice the ALAC that Eric Brunner-Williams has left. And then I'll take it form there with the ALAC call next week. Thank you.

Mikey O'Connor: Okay. I'll forward the note that Eric sent to me to you, Olivier, and maybe that can serve as the notification from the working group. If you need another one let me know.

Olivier Crépin-Leblond: Okay. Thank you.

Cheryl Langdon-Orr: That'll do it.

Mikey O'Connor: Okay onto threats: the continuing discussion. For those of you who haven't been on the last couple of calls what we're doing right now is taking the work that we did in Singapore and basically just combining it and learning a little bit along the way but not necessarily trying to discuss or analyze the work so much as just to get the pieces that people identified in Singapore or on the phone during that meeting into one pile so that we can then start looking at what we came up with.

The meeting in Singapore was remarkably productive and so we're just trying to get it all summarized in one place. And what you see on your screen is the mine map that we've created out of those various subgroups that met in Singapore.

And what you see on the left is the summary, the combination. And what you see on the right is one of the subgroups - the one that (Roya) was described for is still open. And what we're doing is basically dragging things from - just curious I want to take a quick look and see what this looks like - highlight things. Yes so you can still see the highlighting if I move it around, yes. Oh good.

So this is the part that we are pulling from. And this is the part that we're pulling to. And each week I publish a new version of this out on the wiki. So if you look up in the upper right corner of the screen in Adobe there's a link up there if you would like a PDF copy of what's on your screen if it's easier to follow that way. So that's where we're at.

Where we left off was a conversation about the threat of botnets to the DNS and the question is where should we put it. Let me offer one last process thing before we dig into this. And that is last week I felt like I kind of lost control of the call because so much was going on.

And I was having a hard time doing a good job of summarizing people's comments at the same time that I was recording things on the screen at the same time I was keeping track of hands in Adobe.

So if you have a substantive idea that you want to see on this page try typing just a little bit of a summary of it into the chat right around the time that you're talking so that I can just copy and paste out of the chat into this. That'll sort of take the pressure off of me to do a good job of summarizing what you're saying.

So with that botnets if we were to look at the left side of the screen where is a good place to put that? Any thoughts about that? Is that - Greg, go ahead.

Greg Aaron: Well botnets are used for a variety of purposes but the one that threatens infrastructure is DDoS.

Mikey O'Connor: So if we were to take - do we have DDoS in - yes, there's DDoS, all right so we'll put botnets close to DDoS. Does that make sense?

Roy Arends: Hi, this is Roy Arends.

Mikey O'Connor: Go ahead, Roy.

Roy Arends: Hi. Yes that makes sense. There is an additional class of attack from botnets that we see here at Nominet often, Nominet UK. Is that - botnets are used in very large spam runs.

Greg Aaron: Yes.

Roy Arends: And those spam runs result in an indirect attack basically. And sometimes they're so substantial that we see twice the traffic as we normally see.

Mikey O'Connor: So maybe we need two botnets; one under the email spam one as well, right? Is that where you're headed?

Roy Arends: I think so. I think so.

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

Greg Aaron: And I think - this is Greg. I think that we're talking about the load aspects of email which is what Roy mentioned. We need to be careful though of not describing spam as an infrastructure threat perhaps. I mean, it's a problem, it's a type of abuse but not all aspects of it probably are of interest to us or kind of falls under the ICANN mandate. That's all.

Roy Arends: That's - I agree with that. What I - it's basically the collateral damage that results from a spam run that we see that is the threat to the - to our infrastructure. But it's not - spam at large is not a threat to the DNS I think.

Mikey O'Connor: Sure I can spell collateral. That's better.

Roy Arends: Oh great, yes.

Mikey O'Connor: All right that sounds good. I've got load in here. Again I think what we want to do is just capture these thoughts and then clearly we're going to circle back around to this and refine this a lot as we go. Greg, is that it for you? Is that an old hand or a new one?

Greg Aaron: That's an old one.

Mikey O'Connor: Okay. How about cache poisoning - cache poisoning depending on how you like to pronounce it?

Roy Arends: I think cache poisoning is already mentioned on the direct attacks so I think we don't need to - we can - so the two names, Kaminski and (cache purath), those are basically classifications of a cache poisoning attack. There are various variants of those. I don't think we need to iterate over them all. But it's already - yes, it's already listed. Yes, that makes sense. Sorry, I'm trying to read off the screen here.

Mikey O'Connor: Yes and if it's too small I can make it bigger if it...

Roy Arends: No it's fine, it's fine. I have a large screen in front of me.

Mikey O'Connor: Yes, a large screen really pays off on these meetings...

((Crosstalk))

Roy Arends: Yes.

Mikey O'Connor: So it'll help a lot. Okay so that takes care of that one. How about spoofing? Where does spoofing belong in this?

Roy Arends: Yes, to be fair - this is Roy Arends still. To be fair spoofing at the moment of writing on the - on one of the boards during the Singapore meeting spoofing is actually not a threat to the DNS; spoofing is a trick that is being used for instance for cache poisoning. It's due to that DNS is largely using UDP and UDP can easily be spoofed.

But spoofed, I mean, usually an alternate source IP address is sort of the regular one. So I'm not sure we actually should list that, I think it's - it's a trick that people use in an attack.

Mikey O'Connor: Olivier, you want to join in on that or have you got a separate point?

Olivier Crépin-Leblond: Thank you, Mikey. Olivier for the record. I was going to ask actually isn't there another type of spoofing which is used in phishing attacks, i.e. in spoofing of domain names not being the real thing? I know it's on a different level, it's not on the technical level but maybe spoofing might be put in another category as far as threats are concerned.

Roy Arends: One of my thoughts when I joined the DSSA initially is if we talk about the threats to the DNS or to the domain name system are we surely talking about for instance infrastructure, the protocol as such, or do we also talk about the value of domain names and how to devaluate that by using attacks or using for instance spoofing in a way that you just mentioned in phishing attacks?

So clearly that's also a threat but it's all for a different class all together. So I’m not sure if this should be in scope. If this is scope maybe we should separate that from infrastructure kind - infrastructure attacks.

((Crosstalk))

Mikey O'Connor: ...category to put that over here. I don't want to - at this stage of the conversation I don't want to lose any of these. We can sort of figure out the in and out of scope conversation as we go. But for now I don't want to eliminate anything just yet. So if we were to say that these - that spoofing is sort of a different kind of a thing what kind of a thing is it that we can start building a list of them over here?

Just a short phrase that sort of encapsulates what we've just been talking about would be really helpful.

Roy Arends: Yes. Let's continue meanwhile I'll think of something to write and then - and we go from there.

Mikey O'Connor: Okay so I'll leave it over here for now. And then we'll come back. You know, eventually we may discover that indeed this is something we don't want to address but that's way down the road for me in the conversation.

Olivier.

Olivier Crépin-Leblond” Thank you, Mikey. Olivier here. Societal threat I was going to suggest.

Mikey O'Connor: Oh.

Olivier Crépin-Leblond: Now that could be totally out of our scope but...

Mikey O'Connor: Right.

Olivier Crépin-Leblond: ...at least it would be on the other side, it would be on the threat side.

Mikey O'Connor: Yes, let's take that under advisement. Societal, holy cow, another word I will misspell I'll bet. Hey I did it.

Roy Arends: That's fine.

Cheryl Langdon-Orr: Bravo.

Mikey O'Connor: Oh I'll tell you, you are under the command of a guy that can't spell his way out of a wet paper bag so that was a wonderful moment when they invented spell check. Okay so we'll put a question mark by this as a tentative placeholder kind of thing.

That gets spoofing moved over to the sides. All right M&M or M+M; I don't even know what that stands for. Roy, lovely to...

Roy Arends: Yes, I think what happened - I think that that should have read (man) in the middle because of my writing IT looks like a plus.

Mikey O'Connor: Let's take a short pause from hard work to check Roy's picture and just...

Cheryl Langdon-Orr: Oh I like it.

Mikey O'Connor: ...see if we can tell what Roy's handwriting looks like here.

Roy Arends: There we go. IT.

Cheryl Langdon-Orr: In the middle - in the.

Mikey O'Connor: Oh that's what's going on. Okay I get it. All right back to work all of you.

((Crosstalk))

Roy Arends: Oh I love technology.

Mikey O'Connor: Okay so what kind of an attack is a man in the middle? Where does it fit in our little - now note that we have a whole another discussion as to what hierarchy we want to use here and that's another one that we're going to do later. But given all that any - is that another one of the societal ones, sort of like spoofing?

Roy Arends: Yes, it could be. Yes, I think that's a good call.

((Crosstalk))

Roy Arends: It's also in societal as in you basically trick someone to believe you're the authoritative - whatever your authoritative want to be for and basically proxy every information that you get further on. Meanwhile you have access to all that information. That's basically a man in the middle.

Mikey O'Connor: Yes. Yes. Okay fast flux, oh that's an old and familiar topic. Where do we want to put that one? It's probably kind of like DDoS, direct attack kind of things, botnets, kind of in that zone isn't it?

Roy Arends: Yes, the whole idea of fast flux - of using fast flux is to basically make it difficult for someone to find out who owns a specific domain name. You just register a name, you do some fast flux as in you make - basically you erase a paper trail or you try to erase a paper trail if that makes any sense.

Mikey O'Connor: Yes. Well Greg and I at least - and maybe others on the call - were on the infamous fast flux working group in the GNSO.

Roy Arends: Oh great, I mean...

Mikey O'Connor: We have a giant pile of knowledge about that we can bring in at the appropriate time for sure. Okay, operational errors that could be more on the vulnerabilities pile than an attack if that makes sense.

Roy Arends: Yes, it's one of these things that just happen, right? It's not an actual attack...

Mikey O'Connor: But it could be avoided...

((Crosstalk))

Mikey O'Connor: ...during an attack thus might fall in the vulnerabilities...

Roy Arends: Yes.

Mikey O'Connor: ...category. All right supporting infrastructure, you want to expand that a little bit?

Roy Arends: Yes, the - I think this was mentioned by someone else. I just wrote that on the board. And I think the whole idea was that there should be - that - for instance some organizations offer - I don't know, free infrastructure.

How do you call that when you have secondary hosting and you basically use that secondary hosting with closed wallets and basically in terms of - from (unintelligible) you get what you pay for in terms of insurance and that kind of thing so hardly any support. So that - I think it was meant to be a separate class.

Mikey O'Connor: Because we could put it up here in this underlying...

Roy Arends: Yes, yes.

Mikey O'Connor: ...structure. Is that a good place for it do you think?

Roy Arends: Yes, yes, I think supporting - the word supporting is not really valid here. So basically if you use infrastructure you of course need to have proper SLAs and that kind of thing. It's a while back already so I don't remember the conversation vividly but it had to do with, yes, with insufficient support.

Mikey O'Connor: Okay so then if we put it - then I would start to think of it more as a vulnerability but maybe...

Roy Arends: Yes.

Mikey O'Connor: ...that the supporting infrastructure just isn't up to the job. Does that make sense?

Roy Arends: Yes, that makes sense.

Mikey O'Connor: Okay I think what I'm going to do since threats and vulnerabilities are kind of a different thing I think I'm going to make a new category out of that, top level, sort out the spaghetti on the chart later. But I think it makes it easier to understand.

Operational errors - oh no, wait a minute, I'm sorry, hackers.

Roy Arends: In general hackers form a threat to the DNS, right, that's...

Mikey O'Connor: Yes and I would think maybe a direct threat.

Roy Arends: Yes.

Mikey O'Connor: Put that in the direct pile. Homogeneity.

Roy Arends: This is - when you for instance have all of your name servers have the same version of the same kind of software you have - you basically have a very, very small gene pool to pick from. What that means is one vulnerability in that operating system or in that service software could potentially take down your entire infrastructure.

So the idea is in general to have multiple vendors, multiple operating systems, multiple - or redundant locations. So homogeneity is really not good; it's a threat to the Internet - sorry, threat to the DNS.

Mikey O'Connor: Well how about that as another vulnerability?

Roy Arends: Yes, that makes sense.

Mikey O'Connor: Okay, content provisioning exposure.

Roy Arends: I can see from the - from the stuff I wrote on that board that we got more and more tired by the end of the session. I mean, it's more and more cryptic all together. So the content provisioning exposure is - so in general when you have content provisioning for instance if you use Akami or if you use Ultra DNS, one of these things you basically have a login screen and if you leak those credentials to that login screen you have - yes, you basically leak exposure to your whole system.

Rick Wilhelm: Same thing - this is Rick Wilhelm. The same thing happens with registrar account credentials.

Roy Arends: Yes, something like that.

Rick Wilhelm: Yes.

Mikey O'Connor: Something like that. And again this is a vulnerability sort of thing?

Roy Arends: Yes, a vulnerability that can be abused so, yes, I think it's a vulnerability as well.

Mikey O'Connor: Okay. Same kind of thing with the private keys, huh?

Roy Arends: Yes, I think that's a straightforward vulnerability that doesn't need an explanation.

Mikey O'Connor: Okay and then...

Roy Arends: A question from...

Mikey O'Connor: ...there was a question from your group that said what's the perspective of the threat description? And I'm going to sort of segue from that one into Katrina's group because they came up with a taxonomy on that same issue which was that the threat depends on your point of view or at least is related to your point of view. And they have a small diagram that I attempted to reproduce.

Because I think that this whole point of view thing is really a useful...

Roy Arends: Because when we wrote a long time ago the DNSSEC standards we had an accompanying document which was basically RC 4033. And as an exercise for the document what we did is we looked all possible points of attack to the DNS system. So there's one from client, this went from - all the way from application to - sorry, let's start over. All the way from the user to the application to the operating system to the ISP to the authoritative service - sorry, to the DNS system at large and then back to the Registrar/Registrant and so forth.

And all of these notes in that graph and all of these transaction between the notes in that graph is a potential for attack, and I thought it was a very, very good exercise to show the vulnerabilities in the system. Shall I try to reproduce that graph for this exercise?

Mikey O'Connor: I for sure want to make sure I got the right RFC. Is 43...

Man: Yes, that's right. Yes.

Mikey O'Connor: Let's at a minimum take a look at that and see if we could steal things from it and otherwise yes, I think that would be...

Man: That RFC is basically an introduction and requirements to DNS security. Hello?

Mikey O'Connor: It sounds like...

Man: Is that me? Okay, no it's not me.

Mikey O'Connor: And we've got one call that dropped off, but we have our adroit folks from Verizon on the case and they catch stuff like that instantly just as they did now.

Why don't we put this one in our possible taxonomies arena? One of the things that we need to realize is that we're going to...

Man: I'm sorry. Mike?

Mikey O'Connor: Yes, go ahead.

Roy Arends: That - what I - the RFC that I just described was an introduction to DNSSEC, but the RFC that I actually meant to quote is RFC 3833, and that is a threat analysis to the domain name system.

Mikey O'Connor: That sounds like something we need to get right away since - what we're doing right now.

Roy Arends: It's comprehensive. It is fairly elaborate but does not include the things like value of a domain name. It's just on the underlying infrastructure but it's a very good document.

Mikey O'Connor: Okay, I'm going to put one copy of that under there. I'm also going to take this and put it over here as a...

Roy Arends: Mikey I just put the URL into the chat room.

Mikey O'Connor: Oh bless you my son.

Roy Arends: No worries.

Mikey O'Connor: Take that and put that in there too. Terrific. This is exactly what I was hoping would happen - smart people helping your stupid note taker. Okay, that was beauty so we're going to - so having done that, having put the RFC over here under our threats so that we remember to go look - steal the good stuff from there and also putting it under the perspectives hierarchy, have we sufficiently dispensed with this point Roy?

Roy Arends: Yes we have.

Mikey O'Connor: Okay, we're going to...

Man: So from my point of view that is - sorry.

Mikey O'Connor: No, no, you were there and it's really helpful to have somebody who was in the group summarizing it. What I'm going to do is I'm going to do the same with (Katrina)'s group's taxonomy since that goes in the same - make it so I can shrink it.

That should do it. I'm going to put a picture down there. Sorry to mumble. I'm trying to head Cheryl off. She's I'm sure poised to say, "Mikey, you're mumbling again." So I'm sorry.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: Yes. Yes. Yes. Yes I get that. Okay, so now we've got the same, you know, we're still building this possible taxonomy of perspective, and we've got the perspectives in 3833 and we've also got the perspectives that came out in (Katrina)'s group, and we can come back to this at some later point and combine them. Shrink that - yes that goes away. Good. (Katrina), are you on the call today?

Man: She's on - she's working from home, but I'm here.

Mikey O'Connor: Okay, so she can hear but she cannot speak. All right, so I will carry on without her...

Man: She's speechless.

Mikey O'Connor: She's speechless. I've been accused of doing that to people, rendering them speechless. I hope it's not that today. Okay, I think we're going to start to see - what we saw in the other one was we started to see some repeats, and I think we're starting to see that here too, which is compromised credentials we talked about before and we put it up in vulnerabilities. Where did we have it? We had a couple of - there's the credentials one.

Man: Or social networking or whatever.

Mikey O'Connor: Oh social networking. Talk to me more about that.

Man: Or social threat, somebody stealing somebody else's credential.

Mikey O'Connor: The phishing thing.

Man: Social engineering.

Mikey O'Connor: Social engineering, yes.

Man: So it - during our sessions what we did as well might be the low model, the taxonomy model, and then we spent a little bit of time for each one to look at the impact or, you know, vulnerabilities between a Registrant and a Registrar.

If - in here we have like a hacker, right, doing some stuff, somebody hacking the root has a bigger impact than somebody hacking a Registry or a ccTLD. So for each one of the vulnerabilities that we have, there's an impact assessment we should do to figure out what's the impact at the various levels.

Mikey O'Connor: Yes, and I've gone back to your - to the picture that you drew because I think that there may be - for me to - let's see, how do we - so the points at the bottom, 1, 2, 3, 4, are the vulnerabilities in the respective.

So for example between Registrant and Registrar, Number 1 up in the top there. And then the Number 1 corresponding below is compromised credentials is a vulnerability between those two.

Man: So the example here is that compromised credential at 1 would be somebody stealing the Google account with whoever it is, and then going in the Registrar, changing and then hacking their sites.

Mikey O'Connor: Right.

Man: And compromised credential at the Registrar could impact other domains that that Registrar has under control.

Mikey O'Connor: Yes.

Man: And a compromised credential within the Registry, it's like everything for .za for example. And then at the root, well they can change or take it down, right.

Mikey O'Connor: Yes.

Man: So just that single bullet, compromised credential, is for each one of the big buckets as a - the lower you go the bigger the impact.

Mikey O'Connor: Yes exactly. And we need to capture that thought somehow, because that's crucially important. So let me see if I can do that.

Man: So the bullets that we have here, 1, 2, 3, 4...

Mikey O'Connor: Yes.

Man: All of that is covered in the threats and the vulnerabilities that you have. I don't think we need to move that I think.

Mikey O'Connor: Right. What we need to do though is we need to insert the taxonomy in here, so this is Registrant to Registrar.

Man: For each of the threats and the vulnerability that we've identified, we got to figure out, okay, what's - for each of the major component what's the impact?

We do an impact assessment, and then from there we can do mitigation plans later on to how do we mitigate the different vulnerabilities and threats.

Mikey O'Connor: Oh wait, wait, wait, wait. You're going too darn fast. Okay, so we have impacts and mitigation that we need to capture. Meanwhile going back to Number 3 one was Registry to DNS.

The Number 4 one - sorry to jerk your eyes around the screen folks. I won't - promise I won't do this a whole lot. This is DNS to end user. All right, I need to get these pulled into this perspective pile.

Not like that I don't. There, all right. So this is mostly to break the picture out so that we're all text all the time. Then back to the conversation about impacts and mitigation.

I think - do is I'm going to put these in our action items pile because those are things we need to do in the future. I just don't want to lose those ideas. Rick, go ahead. Sorry.

Rick Wilhelm: Yes, I've got - I'd like to add to the discussion. Rick Wilhelm here. I'd like to add to the discussions two papers that the SSAC published in recent years, one called SAC 040 and the other is SAC 044.

They deal with threats and vulnerabilities that - the second one, 044, specifically relates to things about Registrants and actions that they can take to protect domain name registration account.

The first one is related to Registrars protecting their infrastructure and such. So I threw those URLs into the chat room. Both the pages are - both the papers are, you know, pretty readable.

They're not very technically dense and so threw those into the text room for people to read on their free time, copious free time.

Mikey O'Connor: So do we put that down here in the same clump along with the RFC 3833 as...

Rick Wilhelm: Yes, I would suggest that it sort of parallels those.

Mikey O'Connor: Okay.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: Okay, what I'm going to do is I'm going to do a pile of background - put those in there - oh, not that way. Put these in there too. Got some places we can go to check our work and see if we missed anything.

Okay, so that's out of action items to the right spot. Okay so I think we've picked all of the stuff out of this group and put it on her hierarchy. Let's see...

Rick Wilhelm: Mikey this is Rick. I need to drop unfortunately.

Mikey O'Connor: Oh rats. Sorry to hear you're going but thanks.

Rick Wilhelm: Catch up with you all later. Thanks.

Mikey O'Connor: Brilliant contributions - great job.

Cheryl Langdon-Orr: Bye Rick.

Rick Wilhelm: Bye-bye.

Mikey O'Connor: Okay so - bring question mark in the mysterions up in here. Here's a reference to a band that I bet a lot of you've never heard before. Okay, let's see if we can - see if somebody recognizes their sheet here.

Does anybody remember being in this group that could help us? I think we concluded that it was Julie - just blanked on Julie's last name. Who was the scribe? But I'm curious if anybody...

Cheryl Langdon-Orr: Oh it was Chris Wright's group.

Mikey O'Connor: Okay, anybody from that group on the call today that can help me do the summarizing? Okay, well I'll do my usual lame job and - we do - I think we're starting to get into the duplicate area, which is kind of nice.

I think it's easier for me to do it. Poor design, hardware and software - it sounds like one of our vulnerabilities - put it close to the homogeneity one. Okay, natural disasters - we have another one over there so we can put that together.

Now we might have to split this one. Do we have an organized crime? That's a threat. Maybe all of these are threats. I think maybe that's first time for that threat so I'll put it over in this pile.

I'm going to kind of chug along and if anybody disagrees with what I'm saying, just speak out on the call because I'm kind of a long way - my eyes are a long way away from the hands list and I may miss your hand if it goes up.

I think nation states goes in bad players. Implementation errors goes in vulnerabilities maybe up in this zone, fairly close to it anyway. We can - we're also going to...

Man: There's already books in there.

Mikey O'Connor: Go ahead.

Man: Oh I'm sorry. The implementation errors - maybe that's similar to books which is also in vulnerabilities.

Mikey O'Connor: Oh yes, let's pull that up into that same zone - got them together. They're all - these are all sort of related. Poor design, software, yes.

Man: Yes.

Mikey O'Connor: This is all kind of a collection of, you know, there's this operational errors one that is exact - oh well that's a duplicate. So I think scalability is also related as a vulnerability, not so much that people use it as an attack but it provides an avenue for attack if you can't scale.

Rapid change sort of puzzled me. I didn't know what that one was so again I - if anybody is from that group and can remember, we can invent something that says that the operational group at the infrastructure provided Registrar or Registry, whatever, is not able to keep up in which case it's clearly up in this same zone like that.

Process - informal processes again seems like a vulnerability, something along those lines. Inadequate funding also seems like a source of vulnerabilities.

Some of these are almost managerial. Maybe that's the thing. Maybe we do another category. That - okay, how are we doing? We have Olivier's group left.

We are seeing enough duplication and we may get done with this today, which would be pretty neat. Olivier, you want to help place these? Can you see your laptop screen? Have you moved out from your dark glasses or are you still...

Olivier Crépin-Leblond: As I said I'm indoors Mikey. Olivier here for the record. I'm in a cave - not a cave but - right, let's have a look. And now I'm rediscovering these since I haven't seen them since the last time that we spoke, in fact the time that we wrote these.

I think they're quite self-explanatory looking at them and it would be physical threats, which I believe fits in the - there is something on the other side which speaks about this - external events, acts of war, terror, physical disasters.

Mikey O'Connor: Yes over there, right? So if we...

Olivier Crépin-Leblond: We might have a duplication because further down there's also external events and in brackets non-Internet protocol events on the threats.

Mikey O'Connor: Now where's - oh there it is. So maybe we put these...

Olivier Crépin-Leblond: We put these on top, yes.

Mikey O'Connor: All together, yes, like that.

Olivier Crépin-Leblond: They'll obviously have to be refined one way or other.

Mikey O'Connor: Yes, but we'll at least get them close together and that'll put them close together in the outline so we don't forget them. Well that's good. All right, single points...

Olivier Crépin-Leblond: Okay, so the next one is a single point of failure and that is more related to the underlying - I guess it's again the underlying infrastructure, but it's looking at it in a different way.

Rather than looking at any malicious way of doing things we're looking here at a weakness rather than a threat.

Mikey O'Connor: Yes, I think this is more in the vulnerability category. If we could think of vulnerabilities as weaknesses rather than threats which are, you know, things that people do, these are weaknesses that could be exploited by a threat.

Olivier Crépin-Leblond: Yes, so vulnerabilities definitely.

Mikey O'Connor: Yes, and so I think we just put all this stuff kind of up in this same dog for now.

Olivier Crépin-Leblond: And the next one...

Mikey O'Connor: Yes go ahead.

Olivier Crépin-Leblond: Yes, the next one is targeted attacks and again we go denial of service and hacking, and I'm glad to see that we've got man in the middle properly translated and it's not M and M.

Mikey O'Connor: Oh, that just goes to show the difference in my ability to read handwriting. All right, so we'll put that over here because again there's a lot of similarities there. Okay.

Olivier Crépin-Leblond: Now alternate DNS routes was perceived as being a threat and I'm not quite sure whether that is a - that fits anywhere apart - it might be under societal threats. I'm not sure actually. I'd be interested to hear what others think.

Mikey O'Connor: That's an interesting one.

Olivier Crépin-Leblond: Because it becomes more of a political thing doesn't it?

Mikey O'Connor: Yes.

Olivier Crépin-Leblond: Yes.

Mikey O'Connor: Okay I'm going to have to make this smaller. Let me know if your eyes can't handle this. Whoa, very small. Okay too small. Sorry.

Cheryl Langdon-Orr: I can adjust.

Mikey O'Connor: Yes. Yes but after - let's do sort - these all kind of fall together.

Olivier Crépin-Leblond: Correct. The - all three of these are voluntary warfare if you want of some sort that has some political tinge to it.

Mikey O'Connor: Put them in societal threats.

Olivier Crépin-Leblond: Yes.

Mikey O'Connor: I think that's a good parking place for them anyway.

Olivier Crépin-Leblond: I'm not quite sure how the man in the middle turned up as a societal threat. I know there's a lot of people in the middle in politics but...

Mikey O'Connor: Yes. We could move - we could put that up in the direct attacks category.

Olivier Crépin-Leblond: Correct. Yes.

Mikey O'Connor: Put it up in there. Same with spoofing actually.

Olivier Crépin-Leblond: No, I think we had said earlier that the spoofing was not an attack. Spoofing was a societal thing related to phishing.

Mikey O'Connor: Never mind.

Olivier Crépin-Leblond: Sorry Mikey.

Mikey O'Connor: All right, wow look at that. We've moved everything from one side of the page to the other. Aren't we good scouts? I think given the fact that it's five minutes to the top of the hour, we're going to call this a job well done and - yes, to quote a well-known Board member. And...

Cheryl Langdon-Orr: I've got to keep the girl stuff happening, you know.

Mikey O'Connor: Yes absolutely. And I think we'll call it a day. This was a great conversation and I feel a lot better about how it went. I'd - really help all - appreciate all the help in the chat for getting all these little links and ideas out.

That made it a lot easier for me. And we'll pick it up in a week. Thanks folks. That's it for me.

(Andre Sampson):This is (Andre Samson) here. Well done guys and a job well done.

Cheryl Langdon-Orr: Yes.

Olivier Crépin-Leblond: Thank you. Thank you everyone.

Man: Thank you.

Man: Bye-bye.

Man: That was a good session.

Cheryl Langdon-Orr: Thanks.

Man: Thank you.

Man: Thanks.

END