Transcript

DNS Security and Stability Analysis Working Group (DSSA WG)

05 January 2012 at 14:00 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 05 January 2012 at 14:00 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-20120105-en.mp3

Transcript and Presentation will be posted shortly on:
http://gnso.icann.org/calendar/#jan

Attendees on the call:

At Large Members
• Cheryl Langdon-Orr (ALAC)
• Olivier Crépin-Leblond (ALAC) (co-chair)
• Andre Thompson

ccNSO Members
• Takayasu Matsuura, .jp
• Katrina Sataki, .lv
• Roy Arends, .uk
• Jacques Latour, .ca
• Katrina Sataki, .lv
• Luis Diego Espinoza,.cr

• Wim Degezelle, CENTR (Observer)

NRO Members
• Mark Kosters (co chair) (NRO)

GNSO Members
• Mikey O'Connor – (CBUC) (co-chair)
• Don Blumenthal – (RySG)
• Greg Aaron – (RySG)
• Scott McCormick (IPC)
• Rossella Mattioli – (NCSG)

SSAC Members
• Jim Galvin (SSAC)
• Rick Wilhelm, Network Solutions

• Poncelet Ileleji

ICANN Staff:
Bart Boswinkel
Julie Hedlund
Patrick Jones
Glen de Saint Gery
Gisella Gruber

Apologies:
Rafik Dammak, GNSO
Jörg Schweiger, .de (co-chair)

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

Gisella Gruber: Thank you very much. Good morning, good afternoon, good evening to everyone on today's DSSA working group call on Thursday the 5th of January. We have Poncelet Ilelelije, Mike O'Conner, Andrea Thompson, Cheryl Langdon-Orr, Scott McCormick, Olivier Crépin-Leblond, Jacques Latour.

From staff we have Julie Hedlund, Patrick Jones, and myself Gisella Gruber. We have several people who are on the Adobe Connect room. I will read out their names as well as they can hear the audio. We have Don Blumenthal, Katrina Sataki, Rosella Mattioli, Takayasu Matsuura, and Wim Degezelle.

Apologies today noted from Jörg Schweiger and Rafik Dammak.

If I could also please remind everyone to state their names when speaking for transcript purposes. Thank you, over to you Mikey.

Mikey O'Connor: Thanks Gisella, and welcome all to the DSSA New Year's Party, carrying on the tradition. And as always, we'll stop for a minute and let people update us on their statements of interest if there's been any change to those.

Cheryl Langdon-Orr: Mike, Cheryl Langdon-Orr here.

Mikey O'Connor: Go ahead.

Cheryl Langdon-Orr: Not a terribly thrill packed or exciting change to my SOI, but I am now officially a member of another part of the ICANN community. The non-commercial stakeholders group of the GNSO has accepted me as an individual member.

Mikey O'Connor: Wow. Congratulations and welcome to the GNSO.

Cheryl Langdon-Orr: Yes, my pleasure.

Mikey O'Connor: It's too bad you're so unfamiliar with everything that goes on in the GNSO.

Cheryl Langdon-Orr: I'm looking forward to (unintelligible). Yes.

Mikey O'Connor: Yes. Yes. I would think so. That time you spent on the Council I'm sure didn't have anything to do with it. Well, that's great. Congratulations. Any other changes to the statements of interest?

All right, then. We're going to jump right back into the place we left off, which is working our way through the non-adversarial threat sources. And I think we started to slide into a groove. I'm hoping we can start knocking these off a little bit faster than we were. We were sort of inventing methodology as we went, but I think that we're down to the place where we can just do these over and over again.

And so just to replay with a bidding - we've done two of - if you look at this list here. This is our total list of non-adversarial threats sources. We have about I don't know, six or eight. And what we discovered was that it's really hard to evaluate these without also describing sort of where the threat was taking place. The threat event. And so we've - we're combining them.

So we've put two of them together and we have a conversation about any given threat event. And the case that's on the screen, the threat source is a

configuration error by a privileged user and then the event itself is of a - a privileged user of a lesser zone file or one that's not outsourced to a major provider.

And then in that conversation, we talk about two things. We talk about the range of the impact, very sweeping all the way down to very minimal, and we also talk about the likelihood of that impact. And we've done two. We did a major zone file and a lesser zone file from a lesser zone. We have a couple more to do in this category, the configuration errors by privileged users. And then, we have a bunch more types of threats to get through.

So we'll see how we do today. I'm hoping that we can get through a number of these. And Cheryl having no Internet access today due to a big storm which knocked out some key piece of infrastructure gets to vote by voice. For the rest of you, on your screen there is a little polling area and we'll just go through and sort of collect our views, review them, try and talk each other into changing our vote, see if we can come fairly close to a consensus view, and then record that and move on. So that's sort of the plan.

So on the...

Man: Thank you.

Mikey O'Connor: On the hit parade today is the root zone. Configuration errors by privileged users of the root zone. And our first item to vote on is the range of impact if the root zone were to be misconfigured. And with that go ahead and start putting your votes into the little polling thing. We've got one vote so far and waiting for a few more.

(Mark): All right. So this is (Mark). I'm really going to confuse the issue some.

Mikey O'Connor: No. You never do that.

(Mark): Yes, I know. Okay. Okay.

There's two types of configuration errors that actually could occur here. One is configuration errors that are done by each administrator, of which there are 12.

Mikey O'Connor: Okay.

(Mark): And to me, that is limited. That's a limited sort of issue.

Now if it's a configuration error in the root zone itself, then it's sweeping. It's a 10. So there's a different...

Mikey O'Connor: Then we'll make two.

(Mark): Yes.

Mikey O'Connor: (Unintelligible) are cheap. And we'll make a root zone and we'll say - how do you - how did you describe that other one? I've got the individual administrator one in there (Mark). What's the other one?

(Mark): It was a configuration error in the zone file itself. I (unintelligible) zone file that has a mistake in it.

Mikey O'Connor: Okay.

(Mark): Like the (NS set) is wrong for the (Apex).

Mikey O'Connor: Yes. Got it. Okay.

So I'm going to treat those as two different things.

(Mark): All right.

Mikey O'Connor: I agree. I think those are two different things. And so since people are doing the sweeping in the polling, let's treat this particular conversation as the one that (Mark) just told us about. The - this is a configuration error by a privileged user at IANA in the zone that's replicated across all the other servers. And I'm going to...

Cheryl Langdon-Orr: Well that's a huge - what's my biggest number?

Mikey O'Connor: Yes, that's the - off the top. Cheryl, are you on as another sweeping one? So I'll count you as...

Cheryl Langdon-Orr: Oh, I'm right over the top. Yes.

Mikey O'Connor: Yes, okay. So I think we're going to give that one an eight. That's easy.

And then relevance to the organization which we are now calling likelihood...

Cheryl Langdon-Orr: How low can I go?

Mikey O'Connor: I think you can go to - well, our scale goes all the way to zero on this one. One is (unintelligible)...

Cheryl Langdon-Orr: Well look, I never liked the ends of the Bell Curve. Pop me in as a one.

Mikey O'Connor: Okay. We'll put - I'm going to vote for Cheryl, so that'll make my tallying a little easier.

Okay - well I tell you what. I'm going to clear the votes and let you vote again. Hang on a minute folks.

All right, everybody vote again. I'm voting zero for Cheryl. There we go. Now we got the votes where we want them.

All right, so we've got pretty much everybody except Cheryl -- me channeling Cheryl -- showing up as a one. It's described by a somewhat credible source, so we'll give that one seven, and we'll give zero, one, good. I like this pace.

Now we're going to go on to the one that I originally was doing, which was a root zone by an individual administrator, and we'll do the range of impact. Again, this is the sweeping a ten all the way to minimal at one. Wide ranging is five. Eight is extensive. Three is limited.

Cheryl, where do you want to plunk yourself on that one?

Cheryl Langdon-Orr: My gut feeling is more in the three-ish.

Mikey O'Connor: All right, you've got good company. I'll put you in at three.

Cheryl Langdon-Orr: I'm also desperately trying to get my 3G dongle to actually find enough Internet to connect me. At the moment, I'm not even getting one bar, but I will continue to try.

Mikey O'Connor: It does sound like you've had a tough night with that storm.

All right, we've got...

Cheryl Langdon-Orr: Well, I've got satellite connection to all the TV's and everything, so I may even got 3G somewhere else.

Anyway.

Mikey O'Connor: Well, you can watch TV tonight you know, instead of us.

Cheryl Langdon-Orr: I certainly will because I can get to the satellite.

Mikey O'Connor: Yes. Well, we're almost as good as TV.

All right, so now I'm going to do the - clear all our votes out. Now we'll do likelihood and our choices range from pretty darn likely to not so likely. Now this is the likelihood rather than the impact. Where do you want to plunk yourself on this one? This is an individual zone file administrator misconfiguring their file.

Cheryl Langdon-Orr: Oh. What's my range then Mikey? What's your top number?

Mikey O'Connor: Oh, you could be all the way from possible at one to predicted at three, anticipated at five, expected at eight, and confirmed at ten.

Jim Galvin: So Mikey, this is Jim Galvin.

Mikey O'Connor: Yes, go ahead.

Jim Galvin: Just a question. A root zone misconfiguring their file? In principle, they can't misconfigure the file to the extent that they take what they're given and that's what they publish. I mean, I thought this would be about other kinds of operational configuration errors.

(Mark): Well actually Jim, there's two types, and one is actually changing something in (AMD).com. The other thing is -- and this has happened even though root server administrators won't admit to it -- is that they will - something happens and they have to get a zone file a different way and - and they may even edit it.

Mikey O'Connor: Okay. So...

Jim Galvin: So they're not supposed to but they do.

(Mark): And it has happened in the past.

Jim Galvin: Okay. Well then just to make sure that I understand the question then. So this really is about the zone file and an individual administrator and what they do, and we will talk separately about the operation of zone publication, right?

Mikey O'Connor: Correct. I'm making another one as we speak.

Cheryl Langdon-Orr: Well, because individuals can be flakey and stupid and everything else. But can you stick me in a five?

Mikey O'Connor: Yes. I'm giving you a five.

Actually, we're going to...

Jim Galvin: This is Jim again.

Mikey O'Connor: I think we're going to have to redo this vote Cheryl because I - we just changed the ground rules. So hang on for just a minute while I capture the new one that we've done.

Okay.

Jim Galvin: This is Jim again. Just a comment on one thing that (Mark) said when he commented about (AMD).com. I would - I mean at least me, I would consider that still an operational issue, not a file configuration issue with respect to the zone file. If - I mean if you want to disagree with that, I'd be interested in where you want to draw that line.

Mikey O'Connor: (Mark)? What do you think? I'd love to keep it to one thing rather than two.

(Mark): I think it's a matter of semantics from my perspective. The root server administrator has control - administrative control over the entire machine, including the operation of (AMD). So if they want to change (AMD) to a (conf),

or the root zone that they've received from ICANN/IANA, whatever they want to call themselves these days, they can go ahead and do so.

Now whether you call that a system configuration or a root zone configuration, I - you know, I - to me it doesn't matter. It's something that the individual server/operator does for their actual system itself.

Jim Galvin: So - this is Jim again. I agree with you. It's a semantic issue, which I guess is why I sort of pushed the question back just to sort of hear a little bit of perspective from you.

I think the way that I would draw the line is in principle, and administrator, right, is given his own file. And in principle, they shouldn't edit that. They should be publishing whatever they get. Setting aside the fact that they might do things they're not supposed to or do things that they have to in order to make things work correctly.

But everything that they do on behalf of publishing what it is that they get is where I would draw the line, and I would put that on the operational side, and that's why I put (AMD).com on the other side. I'm drawing that clear distinction between what is under their control, or rather what should be under their control versus what should not be under their control.

Does that help any, or change what you're thinking? Or do you agree less or disagree less, or disagree more with me?

Man: I totally agree. (Unintelligible) speaking. I totally agree with you.

Mikey O'Connor: Oops. Let me play back what I've typed. I'm sort of thinking these are two different kinds of things. One is that an individual administrator changes the zone file - the contents of the zone. I'm going to put that in there. And then parenthetically, I'm saying that's something they shouldn't do. They shouldn't be - (relate) to control.

And then the other is - so they publish an inaccurate zone file, but they actually publish it as opposed to the operational stuff where they change something else on their server that means that they no longer publish the zone file at all. How about that for a distinction? Does that help?

Jim Galvin: Or publish it incorrectly for some reason. This is Jim again.

Mikey O'Connor: Yes.

(Mark), how do you feel about that distinction?

(Mark): That's totally fine.

Mikey O'Connor: Cool. All right. So, we're going to vote on two different things. I think we're going to have to redo our range business, so let's just start from scratch. Sorry folks, but this is the nature of this kind of work, which is we learn things as we go and then - so we have to repeat just a little bit. That's no big deal.

All right, so the first one we're going to do is the range of impact on the one where an individual administrator actually changes and publishes the contents of the zone file, which is something they shouldn't ever do. And so our question here is - sorry, I think I may have cleared answers to this one, but go ahead and do it again.

So the question here is what's the impact of that if some - if a zone file in one of the lettered servers is inaccurately published because an administrator changes it? What's the impact on the DNS?

And you know, this is a question that I quite frankly don't know the answer to. If one of the however many it is now, 12 or 13 zone servers has an inaccurate zone file in it, what happens? Do...

Cheryl Langdon-Orr: (Unintelligible).

Mikey O'Connor: Do they crosscheck each other, or do they...

So are - if I'm - if I ultimately wind up at the A server and it's wrong, and everybody else B through whatever it is now is right, who gets impacted? What happens to people doing queries of the DNS?

(Mark): It depends on a whole bunch of different factors.

Mikey O'Connor: Okay.

(Mark): Location. Number of any cast instances. You name it. A typically sees more traffic than the other ones.

Mikey O'Connor: Yes, okay.

(Mark): But that doesn't...

Mikey O'Connor: But if I go to one that's misconfigured, I don't recoil in horror and run off and check a different one.

(Mark): No. You just...

Mikey O'Connor: I just accept it.

(Mark): Yes.

Mikey O'Connor: So I would just question...

Jim Galvin: Is the question about - so this is Jim Galvin. The question about impact has to have a context. So the context is you know, what does it - what is the effect on the Internet, or what are the effects on an individual user? Because on the

Internet, I would argue that the effect is actually pretty limited, okay. It depends a little bit I suppose on the size of the root server operator, but you know in principle, it's pretty limited.

But from the point of view of a user, it's actually quite sweeping because a user typically by default is only going to have access to a particular root instance. And if that happens to be the one which has got bad data in it, then they get nothing or they get all the bad stuff.

Mikey O'Connor: Right.

Okay, so the answer on this one is it depends, and it depends on which server is the one that went down.

Jim Galvin: Well, it matters to the user you know. I mean the user matters. I mean from the point of view of an individual root server being rogue or bad or you know extraordinary things happening, it only affects the limited user community in principle.

(Mark): Actually Jim, it depends on how big the resolver is that caches this, and how many - what is the user population behind that resolver?

Jim Galvin: Okay. So yes, trying to stay at a certain level, but yes. So maybe Mikey said it best when he said the answer really depends.

(Mark): Yes.

Jim Galvin: I think it depends on how close to the user that you are, and that's how you answer the question. The closer you are to the user, the more sweeping the issue. The further away you are from the user, then the less of an issue it is to the user. Maybe that's the right way to phrase it?

Mikey O'Connor: Well - and that gets us to the whole underlying premise of our impact statement, which is what's the impact on the DNS?

Jim Galvin: Right. So for the point of view of the DNS, I think that the effect is actually - well, no. I guess (Mark)'s point actually comes to bear here too. I mean at the point of view of the server, I think the effect is limited. But you know as (Mark) is saying, if you start talking about resolvers, which obviously are part of the DNS infrastructure as a whole, then again it just depends on how big the cache is in that resolver and how many users are tied to it.

Mikey O'Connor: Okay. So we're going to - we have a choice at this point. We could expand the threat tree one more layer on this particular one and say that - would it...

Jim Galvin: So going back to what I said. So this is just Jim again. I mean, I really think it - the impact statement depends on how close to the user you're talking about. I think that's really the answer. The further away you are from the user, the less sweeping the impact or the less dramatic its effect. The closer you are, the more sweeping it is and the more dramatic the effect.

Mikey O'Connor: Okay. So if we were to say - see, I think in order for the methodology to work - I'm not sure. I think what I'm going to do is not record the range of impact for this one, but rather just record that note so that we capture this notion that in this particular instance we want to say it depends rather than trying to nail that down.

The other way to do this would be to actually create two threat events out of this. One that's close to the user and one that's not, but I can see our threat tree then growing sort of infinitely bushy. And I think a better way out of this is just to take note of that.

Now there's a bunch of stuff going on in the chat. (Mark) kicked it off by saying, "One thing I should make clear on this root server zone change is that

this is not been done that I've known about for over a decade," and I think that gets to the likelihood issue.

And then Jim is saying to Jacques - actually it depends. Though Jacques is saying it's one-thirteenth of the user base, and Jim is responding that - by saying, "Jacques, actually it depends on the size of the root server footprint. Not all root servers cover all part of the globe and some do parts more than others. So to say one-thirteenth is sort of over simplifying it." Oh, "And then there's really only one-twelfth, since VeriSign runs two."

Okay. I'm thinking that - okay, let's go on to likelihood, which is getting to (Mark)'s point. Let me clear the - I think - hang on just a minute folks. Sorry this is so halting, but I'm sort of inventing as I go. Something I seem to be doing a lot on these calls.

All right, so we're going to do the likelihood, which I think then gets to (Mark)'s point. Now you can vote how likely do we think that this situation would arise where an individual administrator actually changes and publishes the contents of a zone file incorrectly?

Luis go ahead.

Luis Espinoza: Yes. Luis Espinoza from Doxiar. My comment about likelihood is it must take in account the controls in place to be happen. Then if there's many controls in place to avoid these - one of these mistakes or threats, then the likelihood could be nowhere - should be nowhere - sorry. But if there's no controls, the likelihood to be higher.

My comment is because the likelihood is different thinking in count the controls in place. But I don't know if some of us knows about the controls in place in IANA by example about this management of root zones. That's my comment.

Mikey O'Connor: Thanks, Luis.

And the issue that you raise, which is the quality and capability of the controls that are in place to prevent this actually shows up a bit later in the methodology. And what we're going to do is evaluate those for each of these. And so I'm pretty confident that we're going to be able to pick that up.

But you're right. The tricky thing that we've done by - this is showing up in - a flaw in what Mikey did to the methodology in that the likelihood conversation we pulled forward into this part of the conversation because what we were originally trying to do is just identify the range of impact but not the likelihood. But I've pulled a piece of the methodology forward which I probably shouldn't have done.

And so we may want to treat these as preliminary estimates of likelihood to be confirmed later when we come back around to look at the controls around these things. That's a really good point Luis.

Does everybody else follow my tortured last comment?

Man: Mikey?

Mikey O'Connor: Yes, go ahead.

Man: Yes, about the range of impact, I'm talking about this (whole file) if there's a discussion about this it's only one domain is out and does the domain have flow impact. Then there's a different - there's a difference in the impact in the plate.

But in my perspective this (own) file must be agreed 100% all the time. Then if you - if the (four) parties not accolade 100% all the time then there's a fail in that point of view.

Our own - a few part or only one domain out of the sometimes or restating the (own) file in my point of view is cheated by the threat in this way. Yes this is my point of view of this (unintelligible).

Mikey O'Connor: Right. And in this particular part of the conversation we're talking about the root zone. So this is the zone file that points to the top level domains like .zr.com, et cetera.

So this is not an individual TLD zone file nor is it an individual second level domain like buyer.com. This is the root zone file that we're working on at this point.

Man: Well yes in this matter it is have more - this matter is more - it's important to have the 100% of the accuracy or the (profile). It's not 100 or 100% something failed. And how it failed, you know...

Mikey O'Connor: Yes. Yes, absolutely.

Man: Okay.

Mikey O'Connor: Absolutely right.

Okay so let's do our likelihood think on an individual administrator who's changed and published the contents of the root. That's where the confusion, the root zone file.

So let's see. Let's go ahead and vote. We have Cheryl you want your range? Your range is all the way from possible I suppose number one, all the way up to confirmed and expected, et cetera at ten.

Getting pretty strong support at one right now. Everybody's at one on this one. You want to join the crowd?

Cheryl Langdon-Orr: I am going to join the crowd but I'm also aware that I'm biased by history and perhaps concerns that that's not really taking into account probability of the risk, just measurements of the risk.

Mikey O'Connor: Right.

Cheryl Langdon-Orr: You know what I mean?

Mikey O'Connor: Yes. And this I think gets right back to the point that (Louise) just made which is that Mikey's kind of hosed up the methodology here just a little bit.

I have to ponder whether putting likelihood into this conversation. I think we have to do a preliminary version of likelihood this time around.

Cheryl Langdon-Orr: We need to chew on this - Cheryl for the transcript record. We need to chew on this, me in particular for - because for example if malice comes into it then it's an entirely different answer for me.

Mikey O'Connor: Yes.

Cheryl Langdon-Orr: For our (unintelligible).

Mikey O'Connor: And that's a whole different piece of the threat tree.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: What we're doing right now is inadvertent.

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: If we have a malicious change then we're in a whole different piece of the threat tree.

Cheryl Langdon-Orr: Yes. That's...

Mikey O'Connor: And there...

Cheryl Langdon-Orr: I'm biased by the fact that these things just haven't happened therefore. But I'm concerned that that might be a complacent answer.

Mikey O'Connor: Right. Well and they have happened at least according to (Mark). But they happened quite some time ago.

And so I think what we'll do is we'll treat these likelihood assessments as preliminary assessments. But then when we get to the controls part because we are going to hit controls, we may have to circle back and reevaluate these once we've taken a look at both the controls that are in place and the effectiveness of the organizations at implementing and maintaining those controls.

And that said I think what we'll do is will put this preliminary assessment as pretty unlikely. Everybody seems to be in that camp in the voting. Cheryl, are you okay with riding along on that?

Cheryl Langdon-Orr: Yes. Natural (theatrics) is a really good color.

Mikey O'Connor: Yes actually I'm going to put a note somewhere else on that because what we really need to do is note that these likelihood - okay that's - I started accumulating a Notes portion of the whole chunk of work here. And I think that's where that's going to belong. So we don't put asterisks on all of these because all of these are preliminary I think.

Okay. We've knocked that one off.

The next one is exactly the same except - well it's not exactly the same. In this case an individual administrator changes in operational setting parameter

that removes the zones server from surveying the zone or publishes it incorrectly.

So this is Jim's operational view of the puzzle rather than (Mark)'s. Now hang on folks. I've got to clear. Let me clear our poll.

Right. So now you can start voting the range of impact of an individual administrator changing an operational parameter that removes the zone server from serving the zone or publishes it incorrectly.

And the impact there starting to come in Cheryl in sort of the middle, got some fives, we've got some threes. People are drifting downward towards three, less than impact.

Cheryl Langdon-Orr: Well I'm going to sit in the middle of that rather than below.

Mikey O'Connor: Okay. Hey, Rick Wilhelm's joining the game. Cool.

Rick Wilhelm: Hey guys (unintelligible).

Mikey O'Connor: Great to have you back.

Okay so it's tending to drift into the three-ish zone. Okay I think we've got to - pay no attention to those numbers on the screen. Those are artifacts of the first try or this one at one and six. All right, Olivier go ahead.

Olivier Crépin-Leblond: Thank you Mikey. It's Olivier for the transcript. I'm not an expert in root zone security but I wanted to find - actually the root server security.

I wanted to find out if anyone knows whether a misconfiguration in one of the servers could pose in the others as well or is that something that will just remain in one thanks to that checks that are being done so as to make sure it doesn't poison everything? Thank you.

Mikey O'Connor: I'm going to throw that on to folks who are smarter for me than me. That's for sure.

(Mark)? Jim? Rick?

Man: So configuration we're talking about changes that are to like (Mambi.com) correct to make sure I understand what you're saying correctly?

Mikey O'Connor: No. I think that that was the one we talked about a minute ago. I think...

Man: Okay.

Mikey O'Connor: ...it was the one that Mikey O'Connor the inept administrator of Zone Z, the new most awful zone on the planet screws up his server configuration somehow. And that can mean anything.

That can mean he screws up his backups, he freezes his machine he, you know, any darn thing that you can imagine that knocks his machine of the air or has it start publishing, you know erroneous results.

Jim Galvin: So this is Jim.

Mikey O'Connor: Go ahead Jim.

Jim Galvin: Yes, Jim Galvin. So I'll add the following comment. The thing which is making this hard for me and this question actually makes it hard too is we keep using the word server.

And yet what's interesting is, you know, for most of the root server operators we're talking about Anycast.

So the question really becomes one of - and you would have to believe it's not a really big leap to suggest that, you know, they've got the - so you've got a set of Anycast servers and they're probably managed in some automated or semi-automated way which means if I make an error in a configuration file and I distribute it to my Anycast cloud then sure, I infect the entire cloud and that's going to have a dramatic affect.

On the other hand if for some reason something happens on an individual server that has virtually no affect whatsoever especially if it's monitored and detected in some way, it's taken out of service. Nobody would ever notice and, you know, I mean that kind of thing would happen.

So now we get to Cheryl's comment about, you know, malicious versus accidental kind of issues, you know?

Mikey O'Connor: Right.

Jim Galvin: So I think it's, you know, again this is kind of a hard question to answer because you talk about changing a zone server. But are we talking about individual server or are we talking about an Anycast cluster of some sort? And it matters.

Mikey O'Connor: I think server is of Mikey word and so and because Mikey is so clueless about this stuff. And so I just changed that. To zone cluster over some better word that more accurately.

I mean I think that what we are trying to get at here...

Jim Galvin: You need the word Anycast in there. If we're going to talk about Anycast then we should distinguish it with Anycast. That at least is a known quantity we know what we're talking about.

Cheryl Langdon-Orr: And that is the not (unintelligible) standard but predominant standard that is running at the moment is it not? Cheryl for the record.

Jim Galvin: Yes that's correct.

Cheryl Langdon-Orr: So yes okay. Thanks.

Mikey O'Connor: So if we say Anycast cluster is that a term of art that people will stand up and say I know precisely what we're talking about or have I still got it not quite right?

Jim Galvin: Well I guess, you know (Mark) might have is certainly closer to a preferred term. But one doesn't normally talk about Anycast cluster. The cluster is presumed when you say Anycast. So you just have an Anycast set of servers. I don't know if (Mark) has a preferred term there for that but...

(Mark): How about if I start trying to describe it and maybe we can come up with a term that make sense?

Some of the root servers themselves are not Anycast. And they're all identified by labels. So A is - now is Anycast but it wasn't.

B used to not be Anycast. D for example is not Anycast. So there's - and they're all for the most part administrated separately. So I guess...

Mikey O'Connor: What if we took Anycast out and said - I mean now I'm really hedging the language. But I think this language is really important.

What if we said and individual administrator changes an operational parameter that removes the zone server/cloud/cluster from serving the zone or publishes it incorrectly? That might work.

Jim Galvin: If you go to rootservers.org they actually label it as server which is - and underneath each server they talk about the number of locations you have.

Mikey O'Connor: Rick by the way you should just dive in. You should not be so darn polite. I know that you're a really polite guy but this is really clearly not a polite conversation.

Rick Wilhelm: The coffee hasn't kicked in yet so I'm not - I'm still in polite mode. So this is Rick Wilhelm.

The, you know, the - I think that probably here we're concerned with whether or not the zone is being published correctly or incorrectly.

Man: Right.

Rick Wilhelm: And correctly is fully correctly and incorrectly means any or all of it is uttering incorrect answers or not uttering answers at all.

So largely it probably you could almost instead of saying servers cloud cluster you just say remove the zone - removes the zone from being published or it's published incorrectly.

And how that happens is as (Mark) points out a lot dependent on which root server we're talking about.

So for what it's worth and then on a kind of winding popping the stack a little bit the Anycast cluster is sort of a pretty commonly used term of (art). I don't - not only in my sort of personal discourse but also I did a little Googling you see those two words juxtaposed against each other more often than not.

Sometimes these days they're called cloud but that's perhaps a little bit too trendy for old school DNS folks.

Mikey O'Connor: Yes trendy. I just got a great new domain cloudmikey.com which is where my Apple server sits.

So how's the language looking now? We said an individual administrator changes an operational parameter that removes the zone from being published or publishes it incorrectly. Is that getting pretty honed in?

That neatly avoids all that language about Anycast so that we don't have to...

Rick Wilhelm: Yes and I would say that the likelihood of something like that might be varying based on the points that both Jim and (Mark) made about the use of Anycast versus unicast and a particular operator's root operator's implementation and how they do it.

The probably - you know, the impact is - and but the likelihood of that happening is largely dependent on how the person does it, the operator does it.

That was Rick by the way, sorry.

Mikey O'Connor: Thanks Rick. I'm typing this. So I put that note. I think our likelihood conversation is starting to evolve into maybe this one happens later when we get to controls but I think this is a great place to put these notes for now.

And then we'll - the one thing I don't want to do is lose a key thought. Oh (Rosella) just published a link, technical requirements for authoritative name servers from IANA. I'll grab that one too for the notes. Thanks (Rosella).

Oops. All right so it's seems like we've got good language and we've got a range of impact that ranges sort of in the middle.

Does anybody want to change your range vote before I record them given this clarifying conversation we had? Speak now or better yet change now and then I'll pound these results in to the spreadsheet.

Okay, good deal. I think we're doing a great job although I - we may be at this job until the year 2020 but I think this is really, really good stuff.

Okay so let's see, we've done the right yes I think. Yes we've done that one. So the - let's pick off one more if we can. We've got about eight or nine minutes to go.

One of the configuration errors that popped up was the configuration of a major DNS sect provider. And this is one that I just sort of heard in conversation so I sort of just as before so I rattled it into the list.

I think we probably need a little conversation about this one before we do our ratings because again this is one where we probably want to clarify the description.

And again I'm totally clueless. Are the DNS sect providers typically the same as the organizations that host zone files -, you know, TLD zone files or are they more like DNS providers where they can be completely independent? I just don't know the architecture very well.

Anybody want to give us a small tutorial on DNS sect and how it works? I'm looking to Jim or Rick or (Mark) or any of those smart folks.

Jim Galvin: So this is Jim. A small tutorial?

Mikey O'Connor: Yes a small tutorial.

Jim Galvin: Okay let's see you get a key, you sign your zone and then people validate and you're good to go.

Mikey O'Connor: Okay that's good. So does that mean that there is no such thing as an independent third party provider of DNS sect services? It's all bound up in the zone file conversation end to end?

Man: Hi. This is (unintelligible).

Jim Galvin: No, that's not true. I mean you can even look at what VeriSign is doing now with respect to providing a bump in the wire kind of service, right?

I mean...

Mikey O'Connor: Yes.

Jim Galvin: ...you can just ship their zone file to them, they'll sign it and they'll ship it back to you and then you get to publish it however you would like to.

And they're not the only ones who have that kind of service but, you know, there's is probably the most significant.

Mikey O'Connor: So in that case...

Jim Galvin: You can just have a third party.

Mikey O'Connor: The third party's - the service that they're providing is generating the keys and then handing a file back to you which then gets published whatever way it was getting published before but now it's got the DNS sect keys, correct?

Jim Galvin: I mean I still think the dominant configuration is that you're signing is done by your operator and those two things tend to be tightly coupled.

I still think that's the way it's primarily done today but it's hard to say where all of that's going to go.

You know, I wouldn't even want to venture a guess as to what the most popular if you will configuration's going to be somewhere down the road.

So yes I'm not sure what question you're asking. You know, whoever's going to sign your zone they would have the key.

Whoever is signing the zone would typically control the key. I mean from a security point of view that would really be the only way that you would do it.

Now whether or not they publish your zone for you or they're just providing a service where you give them a zone and they hand you back a signed zone that's just a distinction in service, right?

Man: The market...

Mikey O'Connor: Right.

Man: ...hasn't really evolved to that state yet. Right now if you're capable of hosting a signed zone you're probably capable of signing a zone, would you say that's fair Jim?

Jim Galvin: Well you're certainly eligible to sign the zone if you're hosting it. But I think that not everyone who hosts signs and that's really...

Man: Right.

Jim Galvin: ...kind of the issue that we have today isn't it?

Man: Right, not everyone who hosts signs but everyone that signs hosts. And most of the time if you've got the wherewithal to host a signed zone you also have the wherewithal to sign the zone.

In other words I haven't seen anybody that will host a signed zone for you that won't also sign it for you, right or anybody that could host - like a private person or a company that is capable of hosting a signed zone is almost always - and I haven't seen anybody that is also capable generating that signature themselves.

You know, the long - the high order term in the equation I would say is doing the signing not - and - or being, having your infrastructure - I'm sorry the higher term in the equation is being able to do all the hosting and associate with the signing and things like that, not the actual signing itself. Once you get that wired up it - that seems pretty straightforward.

Mikey O'Connor: So I think that the question on the table and maybe what we need to do...

Man: (Mark) had an interesting...

Mikey O'Connor: ...we've got about four minutes from the end.

Man: ...comment there.

Mikey O'Connor: Oh yes. (Mark) wrote in the chat VeriSign has seen very little demand on their bump in the wire DNS sect service. That's the one where you hand the zone to them they sign it and hand it back, right?

Man: Right.

(Mark): That is correct.

Mikey O'Connor: I think what we need to do between now and next week is ponder what kind of configuration error we want to describe in this DNS sect blob if any and who does it.

This is a really interesting conversation that why don't we just all sort of mentally take a homework assignment.

And my sort of lame chair question to the rest of us is what can a privileged user in a DNS sect environment due to make - to wreck things, to break stuff and...

Cheryl Langdon-Orr: Yes.

Mikey O'Connor: ...see if we can describe that. And then we'll pick the conversation up at that point.

Cheryl Langdon-Orr: And that - Cheryl here. That's going to get us into the - we need to decide what we need to put in the control points part of this analysis and make sure we're certain what we're discussing at this point in the analysis.

Mikey O'Connor: Right, yes. You know, I am starting to realize why the methodology restricted us the way it did. And I'm going to think a little bit about that.

I think again what we're going to have to do is sort of a preliminary pass. You can see why they do these analyses over and over again because the first time you do it you sort of clear out brush and do a lot of hard slogging on terminologies and so on and so forth.

But then coming back through it again gives the chance to sort of refine this. And I think what we'll have to do is park the controls...

Cheryl Langdon-Orr: Listen (unintelligible).

((Crosstalk))

Mikey O'Connor: ...till we get to the...

Cheryl Langdon-Orr: I don't think - I mean I don't feel my time is wasted with this because we're trying to ascertain where the critical control points are and where...

Mikey O'Connor: Yes.

Cheryl Langdon-Orr: ...what risks can be associated with those.

Mikey O'Connor: Yes. No I agree. I think this is really useful. I just know people have the patience to live through it. I sure am glad that we don't have a deadline in our charter.

Cheryl Langdon-Orr: Well...

Mikey O'Connor: Okay that's it for today folks. It's coming up on the top of the hour. I really appreciate all the help and conversation.

Cheryl Langdon-Orr: This is getting to the fun part of the conversation. We're not doing process, we're doing really interesting content and certainly I'm learning a lot during the course of it.

So I look forward to seeing you in a week although I will not be on the call next week. So you co-chair types, we need to figure out how we're going to handle the call a week from today because I have to go to a public hearing on frack-sand mining in my rural district.

So with that I'll see the rest of you in two weeks and have a great day.

Cheryl Langdon-Orr: Thanks Mikey.

Mikey O'Connor: All right...

((Crosstalk))

Man: Thanks Mikey.

Mikey O'Connor: Stop the recording.

Man: Thanks everyone.

Cheryl Langdon-Orr: Bye.

Man: Thanks everybody.

Man: Bye-bye. Thanks.

Cheryl Langdon-Orr: Thank you everyone bye-bye. Thank you very much Jim.

END