BUENOS AIRES – Fellowship Afternoon Session
Wednesday, June 24, 2015 – 17:30 to 19:00
ICANN – Buenos Aires, Argentina

JANICE DOUMA LANGE: …And I cannot believe with my lisp that I actually said that and got away with it. We're going to have different members of the SSR team from the ICANN staff in and out. They all have varying degrees of experience in different aspects of security, but they're all generalists as well that can answer any of your questions.

Steve, I'm going to go ahead and give you the floor first. Steve Conte, which some of you may know from ISOC [fame]. But before ISOC, he was ICANN and he just came back home. Welcome back!

STEVE CONTE: Thanks. I like to call it "MyCANN" please. I don't have any of my other team here. They've left me here to hang, which is why I brought [beer] for myself. John, I think you guys saw John Crain speak on the newcomer session, correct? So I don't want to go over too much about what SSR does. I will slightly recap it, but then I want to open it up and have some dialogue on what's important to you guys as far as security, stability – see, I can't stay it and I work in the department – and resiliency. I mess it up all the time. Means to you.

We look at it from a perspective of I'm going to call it the SSR because I can say that much quicker and easier. We look at the SSR as it relates to the Internet as a whole on the Domain Name System, on unique IP addressing and things like that. We're not necessarily concerned –

professionally concerned – about spam and things like that. Obviously, we're personally concerned with it because I get as much spam as you guys and hate it just as much. But it doesn't really affect the stability or the resiliency of the Internet as a whole.

So we look at things from the perspective of how do we keep a unified and unique DNS in the world and how not to fragment that, because a fragmented DNS could damage the stability of the Internet, because what you expect to go to a website in one Internet, if it's a fragmented Domain Name System, you actually might be going to a different website or a different host. So we look for things like that.

John probably mentioned our work with law enforcement and with public safety services. We help investigate malware. We work with law enforcement around the world to help them understand what DNS does and the tools that they can use to help build their case against bad guys who are doing things and abusing the DNS to do bad things via malware or botnets or malicious registrations, things like that.

We are by no means Internet cops. John might say otherwise, but we're not. We don't personally initiate any kind of search. We assist when we're asked to assist. Especially working with law enforcement and political agencies, we want to be very clear that we are there to assist them, to help them understand what the DNS is or what unique identifiers are and what tools they could do to build the case, just like if they were a cop on the street and they're [walking the case] and somebody steals a car. They need to build that case, so before it gets to a judge, they have the proper things that they could put that bad guy away.

So we do the same thing with them as far as helping them understand what the digital landscape looks like and how they could help build cases to get those bad guys put away.

We do training. I met [Naveed] here through various training. We train on DNS. We train, like I just said, with the local law enforcement or regional law enforcement. We train DNSSEC and we go all over the world and do all kinds of training mostly for ccTLDs that are in emerging regions and to help build that skill set up locally. If there's a need and we can get out there, we like to get out there and help.

I don't really know what to say, so I want to open it up and let you guys talk to me and see if there's anything that I wasn't clear on or John wasn't clear on, or now that you've been at an ICANN meeting for the first week, what does XYZ mean or whatever? I kind of want to keep it as a conversation today. And I'm going to take a sip of beer while you're doing that. Naveed?

NAVEED HAQ: Naveed from Pakistan. I have a question from deployment, specifically from DNSSEC perspective, because people would – I see that [inaudible] to have that. Domains are not signed as – there's recently a statistic about how many domains are signed and all that.

People would say like how many attacks are there in the past 20 years on DNSSEC that would force them to use or adopt DNSSEC. This is similar, not exactly same, but saying that – planes can get crashed, so let's have parachute on board for each passenger. But planes don't get crashed these days. What's your take on that? How to handle the people who come out with such questions? They have a point in that. Thank you.

STEVE CONTE: That's an interesting question. DNSSEC is I think misnamed, first of all. It's not DNS security as much as it is DNS authentication. When you're using DNSSEC, you're not really encrypting a packet or encrypting the conversation between the two DNS servers. You're authenticating that the question you asked to the host and the answer comes back was actually from that host.

Because of that, it's been very difficult to get DNSSEC into the marketplace because there's really no value and no return. Oh, our DNSSEC person is here!

There's been very little value and return to the implementer to put in DNSSEC. How can they charge the customer back? They really can't. There's really nothing to charge them back for because all it's doing is authenticating that the answer came from the host that you thought it came from or it should be coming from.

So even though we have DNSSEC – and Rick, I'm going to let you jump in after I mis-say everything. You can correct me. The more DNSSEC we have, the better it is. But it's not really going to be better until we have applications that are aware of DNSSEC out there. So when your browser is aware of DNSSEC and utilizes it and looks for the special DNSSEC flags and tells you as the user, “Don’t go there. That’s authenticated,” or “Hey, it’s not authenticated,” it’s your choice whether or not to go there. Then it starts to kick in and become more valuable to the end user.

NAVEED HAQ: So the point is how [inaudible] current DNS structure is to have such attacks? How often they occur? I mean, we don’t have stats that support this argument. Every – half of the DNS are not secure, so let’s go for it. Or even 10%. So we don’t have that. I mean, this is something that is – not allowing people to come adopt DNSSEC. Something has to be done on this part.

STEVE CONTE: Yeah, it’s twofold. I agree with you. I’m going to introduce Rick Lamb here in a second, which I actually just introduced. Rick Lamb, everybody.

It’s twofold, because the way I look at DNSSEC deployment and implementation is how can I get my mom to sign the zone without having her really understand what that means? That’s really what the level I think that we need to be at is that when you register a domain and DNSSEC is just part of it, and you say, “Okay, I’m going to generate a key, type in a pass-phrase, blah-blah-blah, and now my mom has a signed zone.” When my mom has a signed zone, Rick has done his job.

Yeah, I know you've got a ways to go. Anyway, Rick is on our team. He is our DNSSEC expert. I didn't want to say that too fast, because that would get weird. But he could maybe address your questions a little bit better than I could.

RICK LAMB: Yeah. Go ahead and ask me questions. I'm sure Steve did a pretty good job covering this stuff. One thing I'd like to say, and if he's covered it, just raise your hand. To me, DNSSEC is not just signing the zones. He already talked about that. Oh, you have a question. Okay, all right.

Naveed, I think your question was without some statistics, we don't know where we are, right?

NAVEED HAQ: The point is we need to convince people how vulnerable current DNS without security is. That doesn't seem to be that vulnerable. I mean, attacks don't happen that often. To banks, we have banking system going on, we have all financial systems, e-government. All "e" things going on. We need to come up with something to convince people to adopt that. That's my point.

RICK LAMB: You're absolutely right, Naveed. You know Naveed. He's a professor and he knows this stuff very well. That is a perfect, perfect point. You're thinking, "Where's the stick that we can smack over people and say this is why you need DNSSEC."

Unfortunately, it’s a chicken and egg kind of problem. It’s very hard to convince people it has any value unless DNSSEC has a certain amount of critical mass deployed. Exactly as Steve said. Until his mom has got DNSSEC deployed – actually, more importantly, your mom’s bank’s website has DNSSEC deployed. Until that happens, there’s not a lot of value.

The flip-side of that – the good news – is that because of efforts like Google, about 25% of the end users in the world sit behind something that actually does the validation, does DNSSEC.

So the only part of the picture that we really are missing at this point is the people who have the websites. They need to deploy DNSSEC. Once they do it, we’re there.

For me, it’s this big pond of pressure that’s building and building and building. Many TLDs have DNSSEC deployed. DNSSEC is deployed at the root. We have these resolvers. Maybe hopefully you learn what that is this week. But the resolvers, the things that actually look names up for you, that’s doing validation. Like I said, about 25% of the people are sitting behind this. But there’s nothing to look at. None of the websites are doing this.

So I think, to answer your question, what we need – one thing is to show the benefits of having DNSSEC versus not. I’d call that fear, uncertainty, and doubt. It’s a term that people use FUD (Fear, Uncertainty, and Doubt).

Great way to sell DNSSEC by saying, "Here's what happens if you don't have it." And there are a couple sites that do this – I should send those links out – that show, "Here's what happens if you don't do DNSSEC."

But for the most part, because so few websites have this, there's no notice. For me, the biggest thing here is it's great that DNSSEC is not deployed. We have now a chance to not only learn, make mistakes. We were very lucky that the gentleman from dot-ke from Kenya, they had a problem a few weeks ago and he didn't want to tell everyone – the world – about how he screwed up, but this is very valuable. This is very valuable information. We convinced him that we want to know what you've learned as we're getting DNSSEC deployed.

So that's the first thing is that by it not being fully deployed everywhere, we have a chance to actually make everything work well. But the most important aspect is this is an opportunity for any entrepreneurs in this space. This is one of those things where it's happening, it's happening, it's happening. DNSSEC is [inaudible] technology, as they say. It's pregnant. It's ready to go.

If you're a business person or you see some opportunities, you see that this is happening, you can start developing those ideas now. I don't know. File patents, do whatever you do. Come up with new ideas that are going to be based on this.

In the US, we have our electric grid, our power grid. There's a whole effort on various companies in the US that manage the power grid saying, "We're going to use DNSSEC to distribute configuration information to your little meters, to electric meters, to everything."

Personally, it's kind of scary. The Internet, power? Oh, my God. Just think something could really blow up here. Nevertheless, there are a lot of efforts like that going on behind the scenes, and to me this is an opportunity to strike and actually do pretty well.

And every time I give the training courses in different countries, my biggest thing is – I live in Silicon Valley or near Silicon Valley. I get sick and tired of seeing the next thing always coming out of there. Come on! It doesn't have to come out from there. It can come out from anywhere. Please, something from somewhere else. I get tired of seeing the same guys doing this.

I see DNSSEC as one of those things where not everyone in the world is completely on board on this thing, but because we have governments and we have this momentum happening, at some point it'll just be there. If you're there at the same time, that's a great opportunity.

Any more questions? He was first, okay.

UNIDENTIFIED MALE: Hello, everyone. I'm going to speak Spanish. Can you hear me? Testing. I'm going to tell you about my experience with Venezuela. I'm [inaudible] from Venezuela.

In Venezuela, we had the support of [inaudible] to create training sessions on concepts and structures for the development of [RPKI], and also workshops at the IPv6 level, so as to facilitate adopting this project [in our] country.

It's been quite useful. It's been coordinated with the government sector to create these skills, and also with institutions within the Internet ecosystem in our country.

My question is how can ICANN contribute to this? It would be very useful maybe to create those training skills or training sessions within sectors that maybe not have such an influence as the government sector and the academia to which I belong. It's so necessary at universities. That's my question or my doubt.

RICK LAMB: Thank you very much for your question. That is a perfect question because, in fact, that is what our team does a lot of. We provide free training, particularly in DNS and DNSSEC.

All you really need to do is ask. And when I say ask, send one of us an e-mail, literally. We would like to see at least maybe 16 people in the room to make it worthwhile. We'll try to arrange to send someone that's not a stupid American. Someone maybe they can speak Spanish would be more effective. Just ask. We love doing this. Maybe as you can hear from my voice here, it's not just about DNS and DNSSEC. When we have these trainings – and I get all emotional about this, so I apologize.

But you get this group of people in a room and you get to know each other. So the different people from the industry in your particular area, city, or region, they get to know each other.

And those relationships can just last forever sometimes. And that's the value. Forget about – I mean, the technology is good and we show you how to do it, hands on. This is all hands on. At the end, you know how to do stuff. I even give people smartcards and equipment. Whatever.

But it's those relationships in the end that I think is, "Wow, just did something good." I don't know. Does that answer your question? Good. Jump in, please.

[STEVE CONTE]: Just to add to that, absolutely talk to any of our team, but a better way to get the word out in the region is to talk to our regional managers. We have Rodrigo here. We have Albert here. Those are the people that we like you to go for when you have a request for training, because that way they can coordinate the regional activities beyond the scope of just the university. They can try to bring more people in and it greater justifies our ability to get down into that region or into that city and do training. I agree with Rick, but please make the first path to our regional representatives.

Actually, I think we have a queue, unless this is a direct follow-up. Is this directly to this? Please, then. Go ahead.

UNIDENTIFIED MALE: I am [Ricardo] from the Dominican Republic. I am a fellow with the Internet Society. I'm not asking about DNSSEC, but something else, so you will excuse me.

[STEVE CONTE]: Was your question directly related to the training or do you have a new question?

UNIDENTIFIED MALE: It's related to some session I went today.

[STEVE CONTE]: Okay. Then we have a queue. I'm sorry. I'm going to let you hold on to the queue. The other thing, as far as training goes, I think we had here, here, here, and here is where we're going right now. We have online training. I'm sure someone has talked to you guys about learn.icann.org. We are looking to contribute to that as well. It's not – it will never…

[END OF TRANSCRIPTION]