SINGAPORE – DNSSEC for Everybody: A Beginner's Guide
Monday, March 24th 2014 – 17:00 to 18:30
ICANN – Singapore, Singapore

JULIE HEDLUND: Good afternoon everyone. This is the DNSSEC for Everybody – A Beginner's Session. We'll probably start in about five minutes or so. Please take a seat at the table. This is a very informal, interactive and fun session, it's not a scary, difficult session. It's probably the funnest thing, I would dare say, that you will attend at ICANN this week, that doesn't involve drinks. We don't have any drinks here, sorry. So at any rate, we'll start soon. Please take a seat up here. We welcome you to the session.

[TAPE CHANGE DNSSEC-EVERYBODY-2]

PRESENTER: …Some of the more recent checks that we've done, it's gotten bigger. It's somewhere now in the 120-175 DNS queries and responses. Any one of those can be hijacked. What's the real purpose behind DNSSEC? It's not to do crypto. The real purpose is to protect the zone content, so that as a user of the DNS you now have a technical basis for actually believing and using what you get out of the DNS. When DNS started nobody was going to go around trying to change names. That was something that wasn't even worried about at that point in time.

The only thing they were worried about was, "Will a silly DNS thing work right?" Well, it did, it worked wonderfully, and now success is I guess

when you get the bad guys attacking you, and that has happened. So DNSSEC is actually the protection for getting correct answers to users. Now, there's a batch of components that are involved in doing DNSSEC. Here's a simple illustration of Joe User, sitting over here. He asks a question. It goes to the authoritative name servers and gets an answer. But before the authoritative name server actually has the data, the holder of the zone, bigbank.com, has to put information into the DNS. So that's the one piece that wasn't in our skit. Somebody else had put it in to begin with.

Now, when you do DNSSEC there's various parts involved, and various ways you can do it. If you're operating some DNS mechanism today, one of the things that I always tend to tell people, and most of the other folks that have been involved in DNSSEC I think have a similar kind of response – you should continue to run your DNS as close to the way you do it today. DNSSEC can be readily added to strategic spots, depending on where you are and what you're doing.

So if you're an operation today that's competent and comfortable running your own DNS, you should probably run the signed version. If you're outsourcing your DNS to somebody else then you want to probably have the outsourced activity do the DNSSEC signing for that particular zone. In terms of user end, like Jacques was our ISP here, doing validation, if you're making use of an external supplier for your DNS operations, then you should have them do the validations for you.

In other words, don't be making major changes to your DNS capability, just because you want to do DNSSEC. So depending on what you're doing, if you're a big, large, registry operation you're going to have

competent DNS people on staff, otherwise you couldn't be a good, big registry operation. In that case, you'll have folks that are already are on DNS – smart, DNSSEC-capable, and they'd be the smart people, in most cases, that you'd want to have do it. If you've got a large enterprise you may or may not be running your own DNS service.

Some of the smaller enterprises where DNS just happens to be there so they can use the Internet, almost certainly does not operate their own name service. So they probably aren't going to do the DNSSEC additional things that you want when you go into the DNSSEC world. Again, the important thing to remember, the blue smoke, so to speak, is you're protecting the correctness and accuracy of your DNS information.

So if you're operating bigbank.com like I was in the skit, I want to have by zone signed, so that it has the blue smoke, so that when Jacques gets the answer he can go through his DNSSEC verification that it was correct and legitimate. So in the simple illustration example we used earlier, it's relatively straightforward. The validating recursive name server has to have knowledge of the key of the root zone.

As Dan was talking about earlier, that can come with the distribution, can be provided by known published places where you get the public part of the root zone. He does the validation. The data that's put into the name servers for .com and bigbank.com just has to be signed. So you're adding relatively small pieces into the overall system, and continuing your operation as much the same as you can for your current operation.

So that's really what I talked about a couple of times. If you're running your own DNS, if you have the skillset in your organization to do it, great.

You should be able to do DNSSEC. If your activity doesn't currently operate a DNS running functionality – if you outsource it to somebody, buy support from somebody – then you need to go to that organization and ask if they provide DNSSEC capability for you. If they don't, gee, where are you going to go to get it?

There are competitive people out there that we're starting to see now; some switching of what's provided for outsourcing to other organizations that do DNSSEC. So that's the end of the presentation aspects. We want to ask people to give us more questions, anything you may have thought of. Please, come to a mic and…

[SPEAKER]: This is [inaudible Zushi? 00:07:02]. I'm from [Sudec? 00:07:06]. This is proven way beyond doubt that DNSSEC is definitely one of the ways to create DNS securely. If it is proven, then why is it still being run as an optional thing, that if you want to choose it you can have DNSSEC? Why is it not just an integrated part of the basic functioning of the DNS? Just like initially when the DNS came up, it had no capability of holding IDNs, but…

PRESENTER: Basically, why aren't we just doing this? Why isn't everybody doing DNSSEC right now?

SPEAKER: I wouldn't do it, because it would cost me more money.

PRESENTER: Well, let's come to that in a second, but that's your question, right?

SPEAKER: Yes, my question is, are there any overheads which somebody may not want to opt into, and that is probably the reason it's been kept optional, or…?

PRESENTER: There are two parts to that really. One of the challenges that DNSSEC has is it's like any kind of protocol that's added on after the fact. You have this bootstrapping issue that you need to have… In the case of DNSSEC there are two aspects to it. One is we talked about the validation side of things; the resolvers that are out there in some way. The picture's here. These resolvers are recursive.

The ISP resolvers have to validate; they have to get the information and validate and turn that on. That's something that… The good news today, in 2014, is that now you can turn that on simply by uncommenting a couple of lines in a configuration file, or running a command on that. A couple of years ago the tools weren't quite up to being able to do that, but today it's a simple matter.

You can do that in BIND, you can do that in Windows server, you can do that in NSD, any of the ones that are being used out there. That wasn't the case before. One issue was the tools needed to catch up and be widely deployed. The other issue is you just have this ongoing thing that a lot of people, for instance in their home networks, they might be using their recursive resolver, which might be at the ISP. It also might be on

the little home router box that they bought for a few dollars from their local electronic supply store.

Those home router devices may not – in many cases are not – set to use validation that's there. So part of the bootstrapping process is getting more people turning on validation. There are a good number of places where this is happening. A number of ISPs across Europe; in the Czech Republic, in Sweden and a lot of the places, all of the ISPs have turned on validation. In North America, where I'm from, ComCast was a big one that turned on validation. Google's done is with their public DNS service, so anyone using Google's public DNS is getting DNSSEC validation as part of that.

So one aspect is you need to get more validation happening. The other aspect is you need to get more people signing their domains, because you need both of them. The people say, "Why should I turn on validation if there aren't a lot of domains that are signed?" and then people are saying, "Why should I sign my domain if there isn't a lot of validation that's happening?" So it's one of those proverbial bootstrapping issues that need to happen. We're seeing a lot of good progress on both sides of that.

We're seeing an increased amount of signing and we're seeing increased amount of validation going on. The gentleman here had a question around… You were saying it costs more money. Okay, here, go ahead.

[AZRIM]: It's a comment for me. My name is [Azrim 00:10:52]. Sorry. I come from a multiple background; for example for designing and helping an

ISP. DNSSEC for some companies would not work because we like to cheat the system. One good example is, "Hey, I want to watch Netflix, or Hulu," or whatever, US programs or football. [inaudible 00:11:18] ISP. So I do DNS masking. DNS masking wouldn't work on DNSSEC.

Because at the end of the day we're spoofing the system to make sure that the [value? 00:11:28] on the other end that we are actually in the US or whatever, despite being in Singapore. So that's one of the reasons. The other end is the [CP site? 00:11:39] equipment, as he says, of course are still donkey years ago, 10-15 years ago? They don't even do this IPv6, let alone DNSSEC. Sorry, that still doesn't work. It's a catch 22.

PRESENTER: Okay. This is the bootstrapping issue; getting both sides of that working. Now, to your point about why some IPSs might not want to do that, there are certain circumstances like hotels, in some cases, Wi-Fi cafes, other places like that, where they do want to effectively do a man-in-the-middle on the DNS so that they can then route people to validation portals. They can do other pieces like that, which does get in the way of being able to perform the secure validation that people want to do.

Now, those are perhaps more [edge? 00:12:30] cases, in some cases, than just the general validations happening. Russ, you look like you want to say something?

RUSS MUNDY: In the US, as Dan mentioned, ComCast has been the leader in doing this kind of validation. In fact, all of the ComCast service in the US is doing

DNSSEC validation. As you might guess, those of us who've been involved in the DNSSEC for a while have in fact had a lot of conversations with ComCast. Frankly, one of the questions was, "How did you make the business case to do that?"

The gentleman there that was deeply involved in doing that had an interesting illustration. That was, "I convince people to do DNSSEC because of the security aspects and because we, as a company, are committed to following the published protocols." So things like hotels or masking or other techniques are actually not following the IETF protocols, and for that particular company that was a commitment they'd made; that they were going to follow the published protocols. So that was one important aspect.

But another important aspect was they were also committed to being a service that was the most security available for their customers. His illustration was every time some of the other marketing people would walk down the hall, and look in this room where they were doing DNS masking or click-counting, and they'd see this big pile of money they could get. I'd have to come along and kick that door shut because they couldn't do that if they're actually going to follow the IETF published protocols.

So he had a lot of battles to fight, and has been successful, and they're still the poster child in the US for who's doing the most. So there are business aspects, and there are equipment aspects. So there's a large number of things. It's not free, and that's one of the things you have to look at, is what are all the costs?

PRESENTER: Question over here I saw. Go ahead.

SPEAKER: You bring up a good point – why it's not part of the regular DNS, right? There are several initiatives that I'm aware of. I represent Microsoft, but I'm also aware of some other initiatives like BIND and some others where default behavior today is not enabled. Default behavior when you create it not signed, so we are receiving serious requests to change that behavior, in order to have more people adopt validation in their recursive layer, and signing in the authoritative layer. We are evaluating that.

When I say "we" I think I should make it clear that it's Microsoft, in those DNS. But we are working very closely with other vendors too. This is not something that I, a single software provider, will be able to solve. We need to collaborate.

PRESENTER: To that point – excellent point – there are a number, for instance, of the Unix, Linuxes out there, like FreeBSD 10 now is coming out, with DNSSEC validation turned on by default. So you're seeing some of that happening out in the Open Source land, in the spaces that are there. I think you'll see more of that happening as more operators go… Okay, I saw this gentleman right there, I think.

[JET THANYA]: Thanks. My name is [Jet Thanya? 00:16:12]. I'm from India, and I'm not from a technical background. I'm just an end user, and I'm a lawyer, so

almost by definition I'm just an end user with absolutely no technical knowledge. But my question is, as an end user, is there any way, and more importantly is there a user-friendly way, for me to know whether or not DNSSEC is in play at any point in time?

PRESENTER: Sure. There's a couple of answers to that. One is that, on a certain level, as users, on one level you shouldn't have to. It should just work such that you should just get to valid websites or you don't. You should just be able to go and do that. Having said that, that's the end game where this is all deployed and it just works that way. Right now there are a couple of different things you can do. There are some plugins you can get for Chrome and for Firefox, that can let you go and see that when you go to a website you will be able to see that. It's called IPFox or…

No that's the IPv6 one. There's a DNSSEC validator from [CZ.NIC 00:17:15] Labs, but they've got one that goes and does that. There's also, on the back of this sheet that many of you had, a list of resources. There's a browser called Bloodhound, that Russ's team has worked on. It's a version of Firefox that does DNSSEC validation as part of that. So that's another tool that's out there.

There are some other people looking at building it into various different components. There is one of these ongoing debates within the application developer community as to how visible DNSSEC should be at all to end users. Or whether it should just fail. The default behavior is it fails if it can't get a good, signed result. So that's an ongoing discussion. Okay, yes?

SPEAKER: [Folly? 00:18:14] from Nigeria. My name is [Bukola Folly?] from Nigeria. I have a question concerning DNSSEC that you're talking about. My question is, will it ever get to a stage whereby everybody will be forced to stay in DNSSEC? For example with the IPv6 thing, the [inaudible 00:18:39] is going on for transitioning from IPv4 to IPv6, and you know for developing countries we are being made to realize that very soon we won't have access to IPv4 and we'll be forced to use IPv6.

Now for DNSSEC, I think what you're saying is that it's dangerous working with DNS alone and not considering the security of it. So [inaudible 00:19:03] to a point whereby everybody will be forced to put the security in place, or it's just a choice?

PRESENTER: That's where the number of us who are here today, providing this session, there's also a full-day workshop, for those who are interested, on Wednesday. There's a session called the DNS workshop that's going on here, where it will be from 8:30 until 14:45. It's actually in the room right next door, the Morrison room, where we'll be having a whole number of presentations and discussions. The agenda's posted so you can see if there are ones of interest to you that are there, but we'll be having some more detailed discussions around this.

There are a number of these efforts that are happening involved. I work for the Internet Society on a project that's trying to do exactly what you're talking about, which is to accelerate the deployment of DNSSEC and get it so it's just the thing that happens, and the people are just

doing [that out of there? 00:19:53]. We're getting a lot closer. We're seeing some very strong trends in the validation side happening.

The New gTLD Program has had the virtue of raising DNSSEC on a lot of people's agendas, because the new gTLDs have to be DNSSEC signed at the TLD level. They have to be able to support it, and registrars who want to sell the new gTLDs have to support DNSSEC, or provide the ability for DNSSEC records to be passed up to the registries to be clear. So you're seeing a lot of that kind of growth. So we're getting to the point where we're approaching a tipping point, if you will, as far as where we're starting to get more focused on.

As I said earlier, the tools have now been catching up too, where it's easier to go and sign, easier to go and do that – across all the range of tools, whatever there might be out there.

RUSS MUNDY: There's one thing certainly that everybody in this room can do to help encourage the use of DNSSEC, and that is to go back to your own respective organizations and ask, whether it's the IT people or whether it's the folks that are running your larger name server operations, when you're going to have DNSSEC available for use in your organization. This has been one of the challenges all along; that from software providers, to ISPs, to registrars, people have said, "Nobody asks about it." So that's one of the important things that everybody in this room can do – go back and ask their respective organizations, "When can I get DNSSEC?"

PRESENTER: Other questions? Right there?

BENJAMIN: Good afternoon. My name is Benjamin, from Nigeria as well. I always mention this is foras like this. When it comes to a place like Nigeria, mobile is really common and strong, and you have developers just going into developing apps. Would DNSSEC put any overhead on what they develop, or are they invisible in this conversation?

PRESENTER: The answer is it depends, certainly on how their item is… It does require a little bit more, because there's another DNS query that has to happen in there to go and retrieve the keys and go and do that. There's a little bit more time that gets involved in that. They also need to be using libraries and pieces that support DNSSEC. The good news is, like the tools, the libraries have now caught up to where they're all now providing DNSSEC.

So there could be, depending on exactly how they're doing it, and what they've got in there, there could be additional processing that they have to do. So there may be some things they have to go and look at. Now, part of it also depends on whether they're actually doing the DNSSEC validation in their application, or whether they're using an external resolver that's out there and doing it. So some of it gets into that space on that.

[inaudible question 00:23:05]

RUSS MUNDY: The other one is a Linux based. They both do DNSSEC on the end phone itself. So those tools are available.

PRESENTER: Yes, it can be done. The good news is there's a good number of libraries. There's also a new library that's being popularized by some folks around here too, that allows developers to get DNSSEC information at a much easier way than has been done in the past. Yes, I saw…? Over here, okay.

SPEAKER: Question. Your statement just now that new registries have to implement DNSSEC. Will the Google [heck? 00:23:54] happen again, given that what happened to Malaysia a few months back. The DNS entries were being hacked, and everybody going to the Google website was being spammed and all that. So does that work or not?

JACQUES LETOUR: Basically what happened is that the Google 8.8.8 name servers got hijacked by somebody else. Somebody rerouted the 8.8.8.8 IP address somewhere else, and they were resolving names on those name servers that were not Google. Right there and then, if anything would have been DNSSEC-enabled, from end to end, then this would not have worked.

PRESENTER: So DNSSEC would have prevented that, because what would have happened is someone would have gone back and they would have gotten responses back and… There's a…

RUSS MUNDY: The client is…

PRESENTER: This is where the recursive name server that was doing validation, the 8.8.8.8, someone got between the client, who did not do DNSSEC, and the validating resolver that did, and was able to fool the client because he was not doing DNSSEC, which emphasizes the importance of getting DNSSEC onto the end machinery.

SPEAKER: [It's not? 00:25:36] something to do with the registry itself.

PRESENTER: No. In one of those attacks it was the issue that somebody had spoofed this, which brings to us a whole separate discussion that we could have around securing the information coming out of the routing infrastructure – a separate discussion that's also being looked at in various different places. But that was a way that people were able to go and say it was somewhere else. Securing BGP and routing and stuff, and pieces that get into there.

Now, Warren Kumari who was here is actually from Google, and he's on the team that looks at… They're concerned about the spoofing of some

of the various different sites that they have, like Google.whatever… Yes, exactly, some of the domains that are in there. Because they… Yes. [inaudible 00:26:19] You're saying the issue here is Google.ny was hacked by somebody else, and this is something Google has been quite concerned about, because those hacks have happened at the registry level sometimes, when people have been able to get into the TLD registry and spoof records there for a registered TLD.

Unfortunately part of the thing – if you compromise at the registry level, or even the registrar level, unfortunately against some of those attacks, if somebody can compromise those servers, they can also compromise the DNSSEC records depending on where it's hosted. I don't want to… I'd be glad to talk to you a little bit more about that. DNSSEC could help in some of those spaces. Yes?

SPEAKER: I was just going to say that when you compromise a registry, when you break the chain of trust, the next level is broken because you are breaking the chain of trust for an upper level. You can delegate from there on, or you can remove any kind of trust from that point on.

PRESENTER: Right. You could remove the DNSSEC records so that…

SPEAKER: What happened in Malaysia, as far as I remember though, I was talking to Warren earlier, was that it was a registry hack. In this case, as you pointed out, there was nothing much that could be done.

[LOUISE NOSAK]: [Louise Nosak? 00:27:43] from a telecom regulator of Vanuatu. My question comes back to how the… I understand that you people are a Working Group on the DNSSEC, but would it help with some contractual obligations like say, for example, a ccTLD manager has a contract with ICANN, and that happens to be an ISP as well, and through that contract some kind of promotion or support for DNSSEC effected into that contract before it's given to the ccTLD manager?

PRESENTER: Yes. There are a couple of different responses to that. Yes, some of the places that have had a large number of domains that have been…

SPEAKER: CcTLDs do have contracts with ICANN.

PRESENTER: Right, correct.

SPEAKER: Not all of them.

PRESENTER: Okay. So yes, so on the ccTLD side there's not a contract with ICANN on that regard. So without wading into those political minefields, the net of it is that there have been TLDs, just to be generic, that have had very successful registration or usage of DNSSEC, by promoting activities for

registrars to go and do that. Now, a couple of the more prominent ones, like .nl in the Netherlands, they've done that through financial incentives.

For instance, they gave a slight discount to people who, if you registered a signed domain, you got a slight discount over an unsigned domain. So they did a few things like that, which wound up spurring a huge amount of interest in some of those areas. A couple of the places have done a lot of areas like that.

SPEAKER: Back to policies, Brazil has passed a law where all the banks in Brazil have to have their domains DNSSEC-signed. That was one thing that also helped adoption.

PRESENTER: In some areas too, in the United States, the US Government specified that agencies, etcetera, had to have their domain names signed. So .gov has one of the highest percentages of signed domains underneath it, because there was a mandate that said that all the government domains had to be done that way. Other questions? Yes?

[SPEAKER]: [Aruwa? 00:30:10] from Papua New Guinea. I just wanted to ask, in the event a registry… If a registrar wants to implement DNSSEC and it's [inaudible 00:30:22] registry has not implemented it, where does that put the registry?

PRESENTER: The question is, if a registrar wants to do this… Let's be clear, because we're starting to get into the funny wording – when we talk about a registrar often, we think of somebody who's doing the registration names, but also somebody who's operating the actual zones. To be more precise, there's a registrar function, which is accepting the domain names and passing the signature information up to the TLD. Then separately there's the DNS hosting operator.

Many times they're operated by the same companies, by the same services. But the DNS operator certainly can go and sign the domains and do all of that. if they can't publish it up to the TLD, then what happens is there's no global chain of trust. It's not linked in there. Now, the domain information can be validated – it will still get a signature back, the recursive resolver could still look at that – they can validate that the information is signed correctly, they just can't necessarily tie it into the global chain of trust, to be 100% sure that it's all lined up in there.

Now, for a number of years there has been a separate service called DLV, which you may heard about, or you may see, that was a way around this, while we were in the process of doing that. That's still out there, but people are not really be encourage to use it, because it's kind of a hack to get around that, that's no longer necessary because we have this global chain of trust. The other aspect is that when you are a DNS operator like that, this is another reason to go to the registry and say, "We want to provide you with DNSSEC-signed records. What can you do there?" I've seen that work in a couple of cases.

ROSS MUNDY: Additionally, if an organization, as an organizational entity, decides that they want to do DNSSEC within their organization, they're in a position where they can do that, even if their parent zone is not signed at all. What they have to do if they're going to do that though, they have to take care of their own key management activity. So if they sign their zone, their authoritative name servers for that zone, we'll give them answers that contains DNSSEC information.

But the machinery that's doing the look-up function for them, the recursive name server, has to also have the trust anchor so they can validate those answers. So it might get them some benefit, but not any connection to the external global scaling.

SPEAKER: I have a question for you.

PRESENTER: Wait, did I answer?

SPEAKER: Yes.

JACQUES LETOUR: You seem more confused than before! You can ask. What is confusing?

SPEAKER: I'm just trying to… In the case of a ccTLD being the [registry? 00:33:45], and the downstream registrar that's hosting domains, the zones – if that ccTLD is not actually implementing DNSSEC, how does that impact…

PRESENTER: Well, kind of to the point you're here… The DNS operator can go ahead and offer the signing, which would provide a level of trust in that you could get back secured answers, but the answers can't be fully validated until the TLD signs. So until the ccTLD signs on that, and starts accepting records from registrars like that, you can't fully get the whole global chain of trust aspect. You can still get the security of DNSSEC at one level, it just can't be fully validated. So in your case, in that scenario, I think you'd need to work with the TLD to try to find out what is their timeframe, what are they doing?

MEHMET: [00:34:50] What's missing, really? What does it take that ccTLD to implement that? is it financial – do you have enough demand? It's all about supply and demand, right? If you can make a business case… Damn, I sound like a corporate guy already… If you can make a…

PRESENTER: The joke here is that Mehmet was with ICANN for a good number of years and just moved over to Microsoft, what, six months ago?

MEHMET: Eight years, yes. Sorry about that. But what I'm trying to say is, if you can make a business case and justify, "Okay, this is the amount of money

we need to spend, but we can charge perhaps some extra for a while so that we can cover those costs. I'm sure… Why would someone say no? That's my question. If you can make the business case. I have a question for Dan. A very hard one.

RAUL [?]: My question is… My name is Raul [inaudible 00:35:45] and I'm from India. My question is, is DNSSEC deployment a one-time activity, or does it require constant updating? Is it an overhead that organizations have to put their efforts on?

PRESENTER: Again, there are two different aspects to that. One is, on the validation side, doing this part, getting the validating recursive, that's pretty much a one-time thing. It's actually the easiest thing on a certain level. You turn on the option in the validating resolvers, you do [inaudible 00:36:18] and lines of code, whatever you have to do. It's a simple thing, you do that and boom! You're starting to do the validation.

Now, on the signing side, there is extra operational overhead that needs to be accounted for. Now, some of that can be automated by the tools that are now available in 2014 that make it so you can go and do it. But for instance, the keys that sign this have an expiration. In this part right up here, the keys that are doing this signing right here, they have an expiration. A lot of the failures that we've had with DNSSEC to date has been because this key expired, okay? The signatures that were out here expired and somebody forgot about it.

Our friends at ComCast will tell you about the experience they had with nasa.gov. They've actually done a really nice write-up about it, that's available out there on the net. They had the case where NASA, in the US, nasa.gov, their key expired and all of a sudden, everybody who was on ComCast could no longer get to NASA's website, because ComCast was doing DNSSEC validation and so all of a sudden you couldn't get to NASA's website.

But everybody could whip out their mobile phone and get to NASA's website perfectly fine because the mobile operators were not doing DNSSEC validation. That created this whole Twitter storm of everybody accusing ComCast of blocking NASA and all sorts of different stuff. When the reality was that the NASA administrators had missed that they had to roll their key. They had to do their key rollover, that kind of thing. So there is an additional operational step that does need to be factored in there.

Now, again, a lot of the tools today take care of that and can make that much more automated so that the process is not there. But it is an operational thing we have to work on. We've got time for maybe one more question, and then we need to…

SPEAKER: I have a question – a good one – but I'm happy to give my spot to someone else.

PRESENTER: All right. Give me your good question.

SPEAKER: It's going to be really hard. Internet Society's doing amazing work, going around promoting DNSSEC.

PRESENTER: I didn't pay you for this.

SPEAKER: He bought me lunch, but I'm not going to talk about that. You guys are doing an amazing job. I want to know, as a part of this community now, how can we help you? You are offering us help, and we want to know how we can help you, so you can help the bigger community, and also we can get DNSSEC implemented. Just to give a little bit of background, I think I would be the happiest man on earth if DNSSEC is implemented, because I was one of the guys that signed the root. So it would be a big achievement for me to see it implemented. But how can we help you?

PRESENTER: Okay, so let's say how can we help the Internet community in general. Thank you for… We do have a site, internetsociety.org/deploy360, and we have a lot of DNSSEC resources that are there. We're also part of this group that includes a whole number of the people that are here, that are working on how do we move this forward, how do we accelerate the pieces that are there. [inaudible 00:39:27]. What? [inaudible] They key for free? Yes, don't charge for DNSSEC. That works for me. That's all, at each level, that the signing happens.

MEHMET: I'm going to extend an offer to people that are operating ccTLDs, and that want to see Microsoft DNS. I'm going to give them it for free, to help ISOC to develop and implement DNSSEC in more regions. You have to be non-profit. Just come and find me. This is something that I can offer here, to support, maybe.

PRESENTER: To be fair, the other tools that are out there, the number of different… I don't know how many of you use some of the tools like [Coco or Fred? 00:40:13], or some of the other tools that are being used for signing ccTLDs. Many of those now have DNSSEC that's available to be turned on there. So you can go and work with that. To answer a much larger question, the big thing we need people to do right now, one of the big things, is to look at this.

Help to explain to people what's going on out there. Turn on validation. That's the one thing we're really encouraging people right now to do. Turn on this part. Get the validating resolvers turned on, so that that way we can see more of the validation happening out there, and we can get people working with that. Then we can start answering this question people have of, "What's the reason for signing this domain?" Where you can, sign your domains.

I'd also encourage you to go and… If you're interested in helping more, there are a couple of good mailing lists out there, and there are some other different resources like online forums, where we're talking about DNSSEC and working together. There's a mailing list called "DNSSEC-deployment" where people get together and they're posting questions around their deployments and the pieces that are there.

We have another mailing list called "DNSSEC-coord" which is about coordination of promotion of DNSSEC activities and things like this. It's also a good time to to point out, on the back of your sheet that you have – and if you don't have one we have a few more floating around –, there are some resources that have some good information about DNSSEC. I just noticed we didn't put "deploy 360" on there, but we'll fix that for next time. There are some tools.

Open DNSSEC is another toolkit that we have out there, that's available to go and help with the signing side of things. The DNSSEC Tools Initiative is a great program that has a whole number of different tools for developers and people that are out there. Some of the other ones… We mentioned… The Firefox plugin you were asking about, that's mentioned here at DNSSEC-validators one that's out there. Bloodhound Browser…

Some other information that's around there as well. I'll mention again, what Mehmet was asking about was the Internetsociety.org/deploy360. So we're coming to the end of our time here, and I know that people want to get together for the gala and for other things like that. So any further questions, comments? We'll be around for a few more minutes if you want to.

MEHMET: Sorry, I've been speaking too much. Just one last thing. Don't be afraid of DNSSEC, okay? It's your job security, literally. It's nothing to be afraid of. I always keep saying the same thing. It's a job security for DNS engineers. They can never fire you. It's going to expire in two weeks and they will hire you back.

PRESENTER: [laughs] Well, okay. But on that note, DNSSEC too, I think one of the key things we want to say here is that DNSSEC is really a way to make sure that you get information out of DNS that's the same information people put in there. It's the way to make the Internet more secure, and we really ask all of you, in whatever ways you can, to help us get this implemented so that we can see a much more secure Internet in the future. So thank you for your time, and please feel free to come up and ask…

SPEAKER: One last question. I asked about the operational overhead that organizations have to get into. From the other end, is there only one version of DNSSEC that is being constantly updated with protocol and the way signing is done, and that gets automatically deployed? How is that happening?

PRESENTER: As far as the protocol development that's there? The DNSSEC protocol was actually developed about ten years ago, believe it or not. It's one of these protocols that's been around for a good while, and now the tools, the other services, have caught up with that. The DNSSEC protocol itself is not being modified too much, the protocol itself, but new things are being offered. One of the things for instance, that we'll talk about on Wednesday, is one of the challenges that we have.

This gentleman was mentioning about the idea of the registrar doing both the registrar function and doing the DNS operator function – doing the actual signing and stuff. That's great, if it's one company, because

they can sign the information and pass it up to the registrar. But if I'm using you as a registrar, but I'm hosting my own DNS and doing my own signing and stuff, the problem right now for instance is that in order for me to get you the DNS key or record stuff that you have to pass up to the registry, for most companies it's copy and paste.

So I have to go into the web interface or the command line for my DNS zone, or my signing. I have to take this bunch of gobbledygook, I have to copy it, and I have to paste it into your web interface, so that you can go and do it. I have to make sure I do it correctly or else I'll wind up with a broken signature, which could cause people not to get to my website. So one of the evolutions that's happening is there are some proposals around that, around how to make that automated, so that as a registrar he could check to see, "Do I have a new key that I need to upload?" and he could take care of that for me.

So it's an evolution like that. But the actual protocol is rock solid. It's being implemented out there. It's being deployed in very large… Millions of domain names are now out there that have been signed. It's happening, it's there. So it's not something that's unstable or uncertain. It's there, it's real, it's going ahead. Now what we're just doing is… Now that we have real operational experience, now we're going back and fixing some of the pieces to go and make sure that it can really work in full operation around that.

Any other…? Okay. Thank you all for your time. Again, for those of you interested in diving into more detail, we'll be up here for a few more minutes, and we also will have the Wednesday session next door, if people are interested. Thank you.

[END OF TRANSCRIPT]