BEIJING – DNSSEC for Everybody -- A Beginners' Guide
Monday, April 08, 2013 – 17:00 to 18:30
ICANN – Beijing, People's Republic of China

JULIE HEDLUND: Welcome everyone, this is ICANN 46 Beijing, China, and you are at the DNSSEC for Everybody, A Beginner's Guide session, and those who maybe haven't come down closer, please come closer because it is really going to be fun and you'll see and hear a lot better if you're up close. My name is Julie Hedlund, I am with ICANN, and when we advance to the next side there will be information on all the presenters and I just want to say I am going to go ahead and turn things over to Dan York from the Internet Society, who is our MC for today.

DAN YORK: Welcome, so first question, how many people can spell DNSSEC? A few of you, all right, okay; everyone else, you're in the right place. This is a session that is a very introductory session. We are going to talk about what DNSSEC is all about, what it solves, the problems that are out there and how it all works. For those who want much more detail there is a companion session happening on Wednesday that is going for 6 hours or so, that gets into the fine details of all of what it is about, that is the DNSSEC workshop that is happening and we have a lot of great information at a great detailed level there, but today we are just going to talk a little about what it is and what problem it solves and give you some good interaction. So here's the schedule of what we are going to be talking about and down there as well too. We have got a fun group of presenters and let me just quickly go down and just introduce who

they are right here. I have Warren Kumari who is here from Google, and he will be one of our presenters and actors in this; Russ Mundy from Sparta; Julie has already introduced herself; we have Norm Ritchie, and we have Jacques Latour coming in at the end there, and we have one other person who will play a role a little bit later. Yes we have somebody who is a plant among you, somebody who will be playing a very evil role in here. So to begin with we want to talk about what this is all about, so we've all heard that DNSSEC started about 10 years ago in the IGF and that may be true, but we have actually got a bit of an alternative history that we are going to give you here, and so we're going to step back about 7000 years and say that the DNSSEC originated back in this time when, we have Aguina, she lives in a cave on the edge of the Grand Canyon. She's there and she wants to see what else is there. On the other side of the Canyon we have Og, and Og also lives in a cave on the other side of the Grand Canyon. And the two of them are there but they don't get to talk very much, it's very hard for them to go from one side to the other, they just can't, it's a very difficult thing to do. So they do get to go and climb down sometimes and climb back the other side and they have been trying to think about how do I go and communicate. So one time when they are there, they see this smoke coming up out of the fire and they just say, "You know what? We could start chatting," so they start doing smoke signals. So here is communication happening in the earlier stages. Now, unfortunately somebody else comes along, this mischievous caveman Kaminski who comes in here, and he moves in next door and he decides he wants to get in on this conversation so he starts sending out smoke signals too. Now all of a sudden Aguina is over here on one side of the Canyon and she was having a great conversation with Og. She was able to go and

have these smoke signals, they had their own system, they knew what was going on, and it all worked really great. And then this caveman Kaminski came along and now he is sitting there saying, "I see two different smoke signals, I don't know which one is real." So they were very worried about this. So one day she decided to go down, climb back up the other side and figure out if she could find out a way to know which smoke signals were coming from Og. So when she was there, she and Og went to go consult the village elders and one of them, caveman Diffy, had a very cunning idea, he knew something that was out there. So what he did, was he ran up and went into the back of the cave and he found out that there, there was a pile of strangely colored sand; blue sand that was only visible there in Og's cave and nobody else had this particular kind of sand. So what he did was he brought that back and he put some of this into the fire, and what happened was the smoke turned blue. Now, all of a sudden, it was really simple because Aguina could be able to look over to the other side of the Canyon and she could be able to look and when she saw the blue smoke she knew that those were the messages that were coming from Og. So when Kaminski tried to go and do this, he would put up his smoke, but it wasn't blue, and so Aguina learned that with blue smoke, she got the right conversation. This ultimately is really what DNSSEC is all about, makings sure that you get the right information and being able to know that it is in fact the correct information you want to have and that is what it is, we are looking for the blue smoke. And now I am going to turn it over to Warren who is going to talk a bit more about how that really works.

WARREN: Great, so in order to understand how DNSSEC works you first need to understand how DNS works. So who here has a good understanding of DNS and how it works? Okay, so some but not everybody. So first off, what is DNS and what does it do? So simply DNS converts human readable names like www.bigbank.com into an IP address that your computer can actually use, like 1.2.3.4, and the way it does this is your computer resolves the name and it does this by starting at the root of the DNS and at each level it asks, "Can you please tell me the IP address for www.bigbank.com?" Or whatever it is looking for, and that level doesn't really know so it sends it on to the next one. So, in this example, you look for www.bigbank.com, the resolver starts at the root and it says, "Hi, I'd like the IP address for www.bigbank.com. Can you tell me? And the root says, "I'm sorry, I don't know that. What I do know is where the .com name servers are, you should go and ask them, they can probably tell you." So the resolver goes along to .com and it says, "Hey, I'm looking for www.bigbank.com, can you please tell me what it is?" The .com says, "I'm sorry, I don't know that but the next thing that's closest to the answer is bigbank.com. I know its address, it's over there, you should go and ask it." The resolver goes back again, goes over to bigbank.com name server and says, "Hi, I'd like the IP address for www.bigbank.com," and the bigbank name servers say, "Oh, wow! I actually know that! The answer is 1.2.3.4," and then your computer goes off and manages to connect to the bigbank web server. So basically in summary, the resolver knows where the root is and it goes along and asks it, and each level in the DNS simply points you to the next level that is closer to the answer and the resolver goes along and tries that level to get to the next one until finally it has the answer. So obviously some names are much more popular that others, like www.google.com or

www.yahoo.com or www.baidu.com. It would be really inefficient for the resolver to each time start at the root and go all the way down asking these questions; it's really long and tiring. So instead the resolver can actually remember the answer for a while; basically it sticks it in the cache and next time somebody asks that question, it has the answer already. And so this has obviously been a whole bunch of information to absorb really quickly and the additional people talking doesn't help any, so we are going to do a quick sort of play to demonstrate this and maybe that will make it clear.

JULIE HEDLUND: Until we get this interference taken care of, we are going to pause and our actors will get into costume, but it is obviously going to be hard for you to hear until we get this to go away.

WARREN: Julie, it looks like my costume was designed for somebody a little thinner that I am.

JULIE HEDLUND: Sorry about that Warren. We are still pausing. Okay thank you very much and then we are going to proceed.

DAN YORK: Okay, so we're going to have a bit of fun. So, it's very difficult to describe DNS and the DNSSEC, it's just a very technical topic, and here we have very distinguished DNS experts and they are going to become actors. So we are going to act out what a DNS transaction looks like,

we'll do different parts, but this is Act 1. So I am Joe User, so I am your typical user, we have here my ISP and then we have the root .com and then bigbank.com. So in this first Act, I am going to be Joe User and I am going to do some banking. So sit down, pay some bills.

ACT 1

JOE USER: Mr. ISP, I would like to go to www.bigbank.com.

MR. ISP: Thank you, but I don't know www.bigbank.com is and the first thing I am going to do is go to the root and ask them where bigbank.com is.

ROOT: Thank you for asking but I have no idea. Why don't you go ask.com at 1.1.1.1.

MR. ISP: Thank you, I'll go ask .com. Do you know where www.bigbank.com is?

.COM: I am sorry, I don't actually know that, but you should try and ask bigbank.com; he's at 2.2.2.2.

MR. ISP: Thank you. Bigbank I am looking for www.bigbank.com.

BIGBANK: Oh, yes, www.bigbank.com! I know where that is. It is at 2.2.2.3.

MR. ISP: Thank you. So now I go and provide the answer back to Joe User, so the address is 2.2.2.3.

JOE USER: Thank you Mr. ISP. Now I can do my banking and my computer now knows that bigbank.com is at address 2.2.2.3 and I can happily go and pay all my bills.

WARREN: So you might be wondering what Dan's presentation or slideshow was all about. Basically Aguina is acting as the resolver and Og as the server, so when evil Kaminski comes along and starts sending smoke signals as well, Aguina gets confused and the resolver doesn't know which set of answers to listen to. And what DNSSEC does is it basically adds the blue smoke to DNS, it provides a way for resolvers to know which is the correct answer. So why is this needed? When DNS was originally designed, there was mainly a scaling problem. The internet was a much smaller and safer place, there wasn't as much need for security; most people knew other people, most people knew everybody else so there wasn't as much chance of somebody being malicious and trying to spoof answers. So the design of it didn't really protect against spoofing, and spoofing is basically somebody pretending to be somebody else, like Kaminski pretending to be Og. And once one of these incorrect answers has been learnt, the name server or the resolver will cache that information, it will remember that information for a while. So DNSSEC

solves this through the use of digital signatures. Basically when you ask a DNSSEC capable name server for the answer, it gives you the next name server in the chain or the actual answer and it signs this answer for you, and then because it is signed you can actually believe it. So now, as well as the resolver knowing what the root name server says, it also knows what the root key is, and the key is basically a little bit of information that is used to generate the signature. And then it builds a chain of trust, so when it goes along to ask the root, "Can you please tell me where www.bigbank is," the root says, "I don't know that. What I do know is where .com is; it is over here. And also I'm signing my answer so that you can believe it." Then the resolver goes along to .com and says, "Can you please tell me where www.bigbank is," and .com says "I'm sorry, I don't know that. What I do know is where the name server for bigbank is" and it signs that, and then the resolver can check the signatures at each level and each level signs the answer to the next one. So obviously that's even more complex than just the description of DNS and so this little skit that we are going to do actually hopefully demonstrates how DNSSEC works.

ACT 2

DAN YORK: DNS is illustrated with Act 1 and what Warren was presenting was how DNS normally works. The DNSO is inherently insecure and we are going to do a demonstration of what's called a man in the middle of a talk and this was the incentive for developing DNSSEC. But right now we will do a repeat of what we did before. I'm going to do some banking again and

	we will demonstrate what a man in the middle of a talk looks like using people.
JOE USER	More bills to pay. Mr. ISP, I'd like to go to www.bigbank.com.
MR. ISP:	Thank you. I don't know where bigbank.com is but I'll go ask the root.
ROOT:	Thank you for asking but I don't know either. You better go talk to .com at 1.1.1.1
MR. ISP:	I'll go there. .Com, do you know where bigbank is?
.COM:	Sorry, no I don't, but I do know that the name servers for bigbank.com are at 2.2.2.2. You should go and ask him.
MR. ISP:	I'll do that. Hello bigbank, do you have the address for www.bigbank.com?
BIGBANK:	Oh yes I certainly do, the address for bigbankl.com is at 6.6.6.6.

MR. ISP: Thank you very much. There you go Joe User, the address for bigbank.com is 6.6.6.6.

JOE USER: Oh, thank you Mr. ISP, now I can go do my banking and pay all my bills at bigbank.com.

DAN YORK: Okay, so that was Act 2 and that was called The Man in the Middle of a Talk, and you can see Dr. Evil here injected the response before bigbank did and that's actually how it works. Now what we will do is implement DNSSEC, and one of the things you might have noticed here is there are two types of servers; one is basically publishing information and the other is reading information, recursive Mr. ISP. So what we need to develop is some way for them to authenticate the information they are receiving. So we are going to have what's called a chain of trust developed and this is what DNSSEC signing is about.

MR. ISP: Hello Root, I would like to do this DNSSEC thing with you, here's my information so that you can believe that I am me.

ROOT: Great, I am now confirming you are you and here is your star.

MR. ISP: Hello there .Com. I have signed my zone, I am DNSSEC enabled at bigbank.com and here is my card to establish it.

.COM: Looks good to me.

DAN YORK: So what's happened there is they have developed what's called a chain of trust, so they have authenticated each other and there would be a digital signature passed between them. So now with the hierarchy signed, we are going to repeat The Man in the Middle of the Talk and we will see what happens.

JOE USER: More banking, more bills. Mr.ISP, I would like to go to www.bigbank.com.

MR. ISP: I don't know where bigbank.com is but I'll go ask the root, I also know that I got this little key here that validates the root.

ROOT: I don't know where bigbank is but I will tell you that you can go to the .com server at 1.1.1.1 and here is its signature.

MR. ISP: Looks good, thank you. I am trying to go to www.bigbank.com, do you know where it is?

.COM: Actually no, I don't, but I do know where bigbank.com is and I can sign this answer for you.

MR. ISP: Bigbank, I need the address for www.bigbank.com.

BIGBANK: Hello, the address for www.bigbank.com is at 6.6.6.6.

MR. ISP: This is wrong, this is not valid data, get out of here!

BIGBANK: Well I am glad you asked. I am bigbank.com and I have the www.bigbank.com address which is 2.2.2.3 and its already signed.

MR. ISP: Oh yes that's good, thank you. There you go Joe User, the address is 2.2.2.3 and it's validated.

JOE USER: Thank you Mr. ISP, now I can do my banking and not have to worry about getting scammed.

WARREN: So as you can tell, we've practised that extensively. And so now I think I'll hand it over to Russ for a sample DNSSEC implementation and guide to deployment options.

RUSS MUNDY: It's always exciting to do this, as you can tell we had a lot of fun with it, hopefully it does help explain the various and sundry activities that are

involved in DNSSEC. Though it is truly when you look at the specifics, there are a lot of very complex details that have to be taking place and happening right, but when you step back to say, "Okay, just what is it that I can do to actually start implementing DNSSEC?" And the answer in almost every case is - Well, it depends on what you are doing with DNS - and so if you are a DNS operator who is really doing DNS as a sort of focal point of their business, whether that is say being a registry operator or being a major ISP and name servers provider and registrar operating a lot of things DNS-wise, then there is quite a few places you can choose to start. If you are a large enterprise type of activity there is also a set of things that you can do but they are probably going to be somewhat different. And so what you need to do is examine what DNS thing to do now, how you do them, and how you fit the new pieces needed to do DNSSEC in, and that is mostly what I'll be trying to cover here today.

And so if you are for instance a registry with big TLD operations, you probably have a professional DNS staff, and in which case you are probably today doing essentially all of your DNS activities with your current staff in-house, probably very knowledgeable, very deeply qualified in DNS things. If you are another enterprise that maybe does important things with DNS but maybe outsources a lot of things, then you've got some outsourced provider that is doing DNS right now for you and you will want to work with those outsourced providers to first of all to establish that they can do DNSSEC because many of them are just now starting to work through the process, and some really haven't started very much at all. If you're an activity that sort of does stuff on the sides, that DNS isn't really the focal part of your business, it's still

important to your business but it is not the main focus, then you may be operating it as a side thing yourself just because it doesn't take a lot of energy or you may outsource it also. And so however you are doing it today, the basic first step is look at what you are doing with DNS things today. If you are like Jacques here and were an ISP, one of my favourite example of some group that has stepped out and done a lot with DNSSEC is in the US, a company named Comcast; it is a very large ISP provider and all of their recursive name servers that provide service to home users are set up and running with DNSSEC today. And so the set of things that they did to get DNSSEC running for their customers are somewhat different than what for instance VeriSign did, who is the operator or .com and .net, when they signed it, or the affiliates did when they signed .org. And so that's really the first step, it's the planning step and look at what you are doing and how you are doing it. If you are an enterprise, HP, big enterprise, big company, lot of DNS expertise, I believe they still do most of their DNS operations in-house, but they do a lot of DNS. And so they are under .com and so they are all set, they can go forth and sign their zone and all of the zones that they have and administer under them. And so however you are doing DNS today is what I am really trying to illustrate here, you need to look and say, "What are the specific pieces?" So if you were an enterprise, you are going to be operating or providing some recursive name servers and you are going to be operating some what are called authoritative name servers or as Norm pointed out, the information providers for your own zones, and so you can be looking at signing of your zones, and in most cases that is the most effective thing to get started first, if you are an operator with authoritative name servers of some sort, just sign your zones. Don't worry about whether or not anybody is doing DNSSEC

validation of them, but get your zones signed first and get used to handling the DNSSEC part of running DNS because there are some changes that need to be made, which is one of the biggest changes in regular DNS. And so the changes that have to occur are on, this is what I call my DNS mountain slide and the left side of the picture is what is often called the provisioning side, and whether you are an enterprise, whether you are a registrar, whether you are a CCTLD, all of these things apply for any given single zone. And on the left side is the place where the information is put in. If you are an enterprise, that may all take place totally within your organization. When you are dealing with your connection to your registrar for like when HP interacts with whatever registrar they use to get to .com, they have to exchange information with their registrar so that the information can get placed in the point of the triangle there, and then it gets used, if you will, distributed and consumed on the right hand side, and if you look at the details you can see there is a lot of players that are involved in that.

And so what you want to do is examine your DNS pieces, know where you get your DNS service today and how it gets done, who provides that service, in-house, IT staff, a DNS specialty staff, outsourced, is it provided by your registrar, it actually can come from a lot of different places. So in DNSSEC planning, finding out where all the pieces are related to your DNS is often the most important very first step you want to take. And so what you see here is another way of illustrating how the skit worked earlier. Information got put in to authoritative name servers and it was asked for by Joe User there and comes back out in terms of an answer.

And it can be looked at simply or it can be looked at in a more complex way. When you look at the top two rows, those illustrate the root zones, name servers and their team letters, but well over 100 machines. Same thing for .com, as you go down there are 13 letters. Then the next page gives you an example of how many resolutions name look-up, or you are asking the question, getting an answer, how many times that can happen. So www.CNN.com, it was at this about a little less than 100 lookups and answers; now when we checked it recently, it is well over 100, it is about 120 now.

So the zone data is what really counts, that's what we were trying to show earlier. It's the IP address for www.bigbank.com, it's not 6.6.6.6, it really is 2.2.2.3, and that's the important thing. That's really what DNSSEC does for you; it provides the technical cryptographic basis that a user of DNS information can take to make that determination and can make it firmly. So you see the triangle picture here again, you notice the green part is where the DNSSEC itself is actually running, which is when you are looking at the left side, that's getting information in, that's the provisioning part where if you are the user of a name and you go to a registrar, the provisioning is all that side, the registrar side. Once it gets loaded into a name server and it has been signed, it's the running information that people go make queries, get answers of, and that's where DNSSEC works. You still have to be very careful on the provisioning side the second place of priority, once it gets loaded and signed people go make queries and get answers up that's where DNSSEC works, they have to be very more careful on the provisioning side, but DNSSEC solves the source authenticity and data integrity challenges, that you get the right information and that it's coming from

the right place, which is a non-security way of saying that for your DNS information. Okay, so if you are doing DNSSEC the same way that you are doing DNS, that's probably the right way to go about it. Take whatever you are doing with DNS today, don't try to throw DNS operations out the door from what you are doing today and replace it with something all new because then you're adding more complexity because you've got to make sure your DNS operations work right before DNSSEC will work at all. This is another illustration with just a few more arrows on it and again from a straightforward how do you get it done, this illustrates the additional places that you need to do some putting pieces in place, so you got our little stars on, that's the arrow that provides the authentication so that the consumer of the DNS data knows it came from the right place and wasn't mucked with as it was going down the wire. So when you are looking at extending your current DNS operations, these are the things you need to look at. The pieces that are putting into DNS and the pieces that are getting information out of DNS and the details of the words, there are more words on the slide that we need to talk about but they are in there so they will be up on the website, anybody wants to see them and talk about them in detail, we can certainly do that, but for purposes of this session I am just going to go on to the next slide, and if your operation is one where your software and hardware products are provided by a group of different things, you need to go to either the vendors or the service providers that are doing the DNS related things for you. Say I need to do DNSSEC, can you help me do DNSSEC, and if they can't help you do DNSSEC, that's when you need to start looking at how you can get your DNS provided by somebody who can help you do DNSSEC. And so the specifics for your enterprise, large provider or professional DNS

operator, you all need to make sure your providers or the products and the services will support. And that is all of our formal presentations. Now we really want to get you people out there to ask and comment on what you've seen. If you have things that you think were just totally stupid or off the wall, tell us and we will try to explain it but we really want to answer your questions, and as much as anything that is really what we are here for today, is to be able to answer questions you might have, because we have got folks with mikes.

AHMED: This is Ahmed from Pakistan. My question is how much it will slow down the overall traffic of the internet? Will it affect or not?

RUSS MUNDY: The short answer is basically not at all. You get the signed answers when you do your normal DNS queries. The answers are slightly bigger, but it is still a very, very small amount. There is a tiny bit more processing, but when people have done benchmarks it is on the order of less than a percent, and that's just for the DNS part, the rest of everything is not affected at all, so in the total scheme of things it is completely negligible.

DAN YORK: One thing that we do have some fairly good studies on is on the impact on authoritative name server providers, and a very effective analysis was done by Wright a few years ago and the analysis is still pretty good, it is available online, lots of formulas in there, lots of specifics, so for an individual zone you can grab that report. Plug your numbers in and find

exactly what it will do for your particular environment in terms of authoritative name servers. Now we don't have as detailed a data available on the validating resolvers. Warren, have you gotten anything back from the Google DNS guys?

WARREN: No public data that's been published but it is the sort of numbers that get lost.

RUSS MUNDY: There are a couple of other groups out there trying to measure the validation side of things and likewise I have not heard of any kind of significant impact right now.

LENDAL MCDONALD: I'm from the fellowship program. How costly is it to implement DNSSEC?

DAN YORK: So I guess the question goes back to sort of "it depends" to Russ's point, it sort of depends on how you are, how big your zone is, how involved your system is. Actually Jacques just went through some of the process with .ca and he can perhaps talk a bit about it, but it also depends on the level of security, the level of caution you want to put around your whole environment and what you do and there is a wide range. There are people who have done the signing and doing some of the different pieces with a variety of open sources and other components and things and at a very minimal cost versus other people who have done very large scale environments with hardware assisted key encryption and

separate lock-down rooms and lots of things where there is a huge cost involved, so it can range in that. So I'll turn it over to Jacques.

JACQUES LATOUR: It depends on your security requirement, so if you are a CCTLD or an operator or a business and that defines basically how much you are going to spend. It can go from zero, all open-source software to very expensive.

WARREN: And I think that there have been a number of CCTLDs that have done this for basically zero. There is some time investment to learn how to do this and to make sure you are operating in a stable manner. I mean even CCTLDs which are relatively complex environments have done this with one guy, a few days stuff, and then no actual cost. If you are just an organization wanting to do this for your own use, you could fairly easily do this with no cost at all.

DAN YORK: To go into the organization side of things and build up what Warren said, a lot of the existing authoritative names or pieces that are out there and on the resolving side as well, the code is already there and turning on DNSSEC is a simple matter of often just checking your box or adding one line to the configuration file. If you are using any of the standard bind or one of those Microsoft Windows Servers, or any of those kinds of validating resolvers, it is a simple matter of going in and adding a line to the config file, it is already there on that part on the validation side.

RUSS MUNDY: One thing I'd like to add in particular for this question is that, as I said in the presentation, it is really the data, the content of the zone that is important, that is really what you are trying to protect, and so you should expend the effort that is roughly reasonably equivalent to how you protect the data in the zone itself. And so if you have a fairly easy loose process for people adding and taking names into and out of your zone, making changes, don't get a lot of attention and scrubbing for accuracy or maybe just a minimal check, you don't want to spend a whole lot on DNSSEC because you are then spending more money on the crypto parts than you are on protecting the content parts.

LEON: I'm Leon from the fellowship program as well, and I've got two questions. First one is using Google's public DNS server gives me like a bulletproof certificate for surfing the web? And the other one is how can I as an individual that owns a couple of domain names, contribute to strengthen the DNSSEC?

WARREN: So Google has recently started doing DNSSEC on the Google open resolvers, but it is still on sort of a soft launch phase. This means we are only giving signed answers if people specifically request them; if people specifically request the DNSSEC stuff then we will give them a DNSSEC answer. Sometime in the future and in the fairly soon future or near future, we are planning on turning this on for everybody. So basically if you ask 8.8.8.8 a query for www.bigbank.com it will give you back a DNSSEC answer. This is similar to what Comcast is already doing. If there is an especially large zone, like this happened not too long ago for

nasa.gov; they accidently messed up their DNSSEC keys and so the zone wouldn't validate and nobody could reach it who was using a DNSSEC server. Comcast put in what they called a negative trust anchor and they said even though this doesn't validate we have checked and we know why it doesn't validate, so we are still going to give an answer. It looks as though Google will be doing the same thing if it has become clear that the reason that the zone is not working properly is because of just a temporary mess up or you know the person who does the signing went home for the day and forgot to do stuff, it is possible that they will still give you an answer even though it is not actually DNSSEC secured.

DAN YORK: I'll talk about what individuals can do because there are some very easy things that you can do. One step is if you own domains, sign them, and now when I say sign them it will depend upon whether you can. There are couple of factors. Of the 300 some odd CCTLDs and generic top level domains, about 100 of them are actually signed, so if you are in one of those 100 then the good news is that from the top level on down your domain can be signed and you can go and make that work. If you are in one of those, the next step is you need to find out if your registrar will support DNSSEC, and in some cases they have automated it down to where there is just a simple checkbox that says Enable DNSSEC and you click that and you are protected. In some parts of the world there are registrars that just do it automatically, like Netherland and other places. If you are using .com, .net, .org or one of those, you need to find a registrar that does that and there are a number of them out there. ICANN actually has a site on a page on their website that lists the registrars that support DNSSEC right now. And so as an individual I have

gone to those registrars, I've churned out my domains and in a couple of cases there were some that I had to ask my registrar and say when am I going to get this, and in one case I moved a domain to another one out to another registrar because I wanted it signed. So that's on the signing side. On the validation side, it depends on how involved you want to get, what you want to do, what your level of tech savvy is and all that. There are some tools, I run one on my Mac, there is a program called DNSSEC trigger which is made by the folks at nlnetlabs, which gives me a validating resolver on my own system and so I can use it and instead of the ISP doing the validation my local computer is doing it. And so it is one that I can configure to use Google's public DNS servers right now, and so when I'm running a software on my system it will then go and query Google's system. So those are really the two things you can do, which is you can either sign your domain on the signing side and on the validation side you can find out if your ISP or whoever provides that, if they are supporting DNSSEC and if they aren't, ask them, and then if you want to get into it you can go and install the software there. There are also a couple of add-ons for Chrome and Safari and IE that will go and provide some validation signals there as well.

JULIE HEDLUND: Just so we have a queue, there is a gentleman over there and a gentleman here, and now I saw another hand up there and another one, so we have four in a queue.

DAN YORK: One more quick addition, if you are operating your own names, the name servers for your own names, and you don't have a chain all the

way to the root, you can still sign it. There is nothing that prevents you from doing that. Now other people won't be able to validate down to you unless you provide them your trust anchor, but as far as having names and operating it yourself, you can learn and incorporate into your processes right now DNSSEC for authoritative sign zones, whether or not you've got a chain all the way to the root. And there are a number of capabilities, DNSSEC trigger is a very good one. So there are tools out there today for doing DNSSEC validation. I urge everybody to grab them and try and use them and give feedback to the developers.

RUSS MUNDY: The paper that you have should have some URL on it, so you could follow those and check those out.

QUESTION: I'm from China. I have two questions. The first one, do you have any data that shows how many servers or the rate at which servers have employed DNSSEC? And the second one is if a DNS server is controlled by hacker, could DNSSEC still be useful in this situation?

RUSS MUNDY: To your first question, there are a number of different data points. Probably the easiest one is to see the deployment in the CCTLD world, so there is a map that was on DNSSEC deployment that's on deploy360 site that actually will show over time the number of CCTLDs that have been signed. There are some counts otherwise but that is probably the most visible way to illustrate the growth so far, is by looking at the CCTLDs that have been signed because the map does show it to you

over time. So you can get an idea of the growth also. Now if a hacker controls a name server, with DNSSEC, what is actually being authenticated to the end user that is using the DNS information, is the data itself, not where it comes from in that exact machine that is sending you the bits but where it comes from is the originator that put it into the DNS, and so if it is one of the other name servers in the middle somewhere that may have some information they are either spoofing or they somehow got some wrong information, they cache and they give it to a validating resolver, that validating resolver will detect it and say no, this is bad data. If the hacker were able to get control of the machinery that was doing the signing, so yes they could cause damage there. If they got into the provisioning side where the data is going in and they put that data in before DNSSEC was applied, then the bad data would be in there and signed by DNSSEC and in that case the validating resolver wouldn't be able to tell because it would be signed and the weakness is in the provisioning side, so here is the map.

DAN YORK: This is a map that is put together by the folks at a company called Chinkura, they have been publishing these maps for bit and this shows the adoption going on, both the operational but also the experimental and on the website where Warren pulled this from, there are a number of other maps based on each region and also there is an animated gif that kind of shows the trend over time. I would also say on Wednesday, if you get a chance to come to the DNSSEC workshop that we have, there is actually a series of talks that will be specifically talking about trends and at the beginning of it. One of the folks involved is in this room, but he will be talking about some of those trends and statistics

that have been happening over time, so we will have a deeper dive on that then.

JULIE HEDLUND: I just want to note, this graphic for those who are not in the room we would recommend that you go and look at the presentations for the DNSSEC workshop on Wednesday, because that particular graphic that we were talking about just now was not showing up in the Adobe Connect room, so if you were wondering what we were talking about it is a map with colors on it showing levels of DNSSEC deployment and there will be more on that on Wednesday.

RUSS MUNDY: Thanks Julie. Okay, next?

MOHAMED: Hello, my name is Mohamed, I am from Bahrain. I would like to thank you for the comprehensive show, I just have two questions regarding the DNSSEC. What parties are involved in the DNSSEC transactions, is it long way to the end user or let's say from registry and I want to implement the DNSSEC. Well the end user in sense something new or he needs special configuration on his laptop. This is the first question, the second one is why there is signing or signature between the root and the other sub-roots, because I think they are well defined, so as you demonstrated earlier these roots should be well defined and if I say as a root for the ISP go to the dot com, why I should sign this transaction if the dot com server is well defined?

RUSS MUNDY: Let me answer the second question first. The DNS by its nature if you remember some of the slides one had starts from one spot and then works its way down, and that's the information structure of the content of the DNS, so every request of information for DNS output, resolver of some sort of kind, knows where to start and any resolver that's doing a lot of work and lot of fetching, it is called recursion, cursive resolver it knows where all the root name servers are, but it doesn't have known anything else and you know there is single box for the root there are actually a large number of machines that can provide you that answer, so since the DNSSEC by its design is intended to be an integral part of DNS that was the reason that the design decision was made that the information that the essentially is the rough equivalents of, I know where the IP address of the root name servers are, I know what the published key for the root zone is and just like they start for walking down the tree with their queries, they start with the published key for the root and walk that down the tree also, so it's basically to be parallel without the name system itself is structured.

DAN YORK: There is a simpler answer which in a sense is Dr. Evil over there could present signatures, because he could go and sign the zone something like that and presenting would like that, but we have got the global chain of the trust from the root down that ensures the ISP or whoever is doing evaluation, when they look at that they can go and check that all the way back to root like Russ talking about. So that's what I and you need that kind of chain, so that the attacker is trying to give you something that the attacker says is signed and you can go and check

that signature and say well no wait, that's not the signature that you are supposed to use.

WARREN: So you need to answer that in another way, we have three ways of answering. So, the way the signatures work is public cryptography, so in that you have a public key and a private key anything that signed with the private key can early be scripted with the public key and that sort of the signing with private key is same as in scripting the signing key, private key is the same as signing key. So, when you go to the roots, they root says I know the answer for I don't the www.bigbank.com is, I do know where dot com is though, here is the public key and here is my signature saying that it is correct.

MOHAMED: Why don't the root servers give the IP addresses or not signed, not with the key, just because they are well defined?

WARREN: What, the dot come servers are well defined?

MOHAMED: The dot com or dot org or whatever?

WARREN: Well there are lots of different TLDs and so the dot com ones are well known but when you launch a new TLD that won't be known yet.

MOHAMED: Yeah but you should have a pool of all of them defined I think so?

WARREN: Basically there is millions and millions of resolvers and only one root zone, now 13 addresses, but that way the millions and millions of resolvers only basically have to know one set of addresses, they don't have to know 100, they don't have to know 1000, they don't have to know a million, there is well over a million zones, and so since resolvers already had to know where the root was starting and having the root sign, there is nothing that prevents you similarly from having other keys that you know and don't have to validate the root, if you trust those keys, of course you are an enterprise, or a country whatever and you want to have all resolvers in country and enterprise have the public information key part and your resolvers ever have to go beyond the environment they can prove right from that, but its more complex the bigger that gets, so keeping it small to just region was considered the best approach for the global internet, but similarly it does not prohibit a structure where you would have, they are called sometimes trust anchors, for a smaller local area.

DAN YORK: Could you repeat your first question because I think we've lost that.

MOHAMED: I was asking about which parties are involved in the DNSSEC transactions, is it going all down to the end user?

RUSS MUNDY: Policy is always important and this is ICANN so we must talk about policy. There were a bunch of arguments earlier on in DNSSEC activities about is there a need for a common or ubiquitous policy and the conclusion in the technical design and the ITF community was no, we are going to tell you how to do all the technical cryptographic protections, but the statement or the requirement for what has to be the policy that runs those is really beyond the scope of the technical definition, so there are quite a number especially the rezone and many of the CCTLD's, they have issued policy statements and says our signature on our zone means this and it will be operated in the following way, but that's not a required or necessarily integral absolute necessity of having a DNSSEC zone signed.

WARREN: As with all questions that involve ICANN and policy the answer is a little more complex. Russ was mainly talking about on the provisioning side the resolution side at the movement is usually the people involved are the service that they had the signature and the ISP resolver. Currently, the end users machine is not in general doing very much with this information, but a lot of people think eventually the end users machine will also be involved and so the DNSSEC resolution or the DNSSEC validation part will happen on your local workstation.

DAN YORK: I will just add on that. You are seeing now some people are building that resolution into the actual applications that are there and so there are people who are doing DNSSEC validation inside the apps, other people are looking at ways to add it to the operating system and I think to

Warren's point, we are seeing a stage roll out, we are seeing right now that the ISPs are doing a lot of it and then over time it will be pushed down more into the edge and into the operating systems and pieces like that as we get more of that.

DAVID MORISON: I am David Morison from New Zealand registry. We've got DNSSEC signed and working. I deal a lot with the registrars. We have got about 4% of our registrars digitally offering DNSSEC and the DNSSEC is obviously in place for good reasons, that's been done for public good. When I have a conversation with registrars it is more about recent demand, why should I be implementing, so I'm interested in knowing what sort of things might be being done to help educate the general population and add more to the demand side so that registrars can understand the benefits of adopting DNSSEC.

DAN YORK: I will answer that because that's a program that I am involved with at the internet side where we are very specifically looking to try to do this and to drive the demand and to work with that, and so over the past years we have been ramping up this program that I am part of. You are absolutely right, it is the proverbial bootstrapping, chicken and egg type of situation where we need to go and get a demand, we have this problem probably more people say why I shall rule out the validate name service because there is not lot of demand and in the opposite side we have people saying why should I sign my zones because there is not a lot of validating resolvers out there. Now I'll be honest and say that I think my colleague down here at the other end of the table has

helped a lot with that and necessarily you personally, but Google's endorsement of that was a huge step because it certainly got a lot of people talking about Gee maybe we should be paying attention to this because Google thinks it is important. So, quite honestly I think that was a big step that has helped, I have already seen it both in the traffic to and the enquiries we've been getting around that. One of the things you will hear about in this workshop on Wednesday if you come to that, we will be talking about some of the different use cases and some of the different things with people using it. Russ referred to something called Dane, which is a mechanism for basically upgrading security of the certificate system that we use and providing additional layer of integrity, a layer of assurance of the SSL certificate, the TLS certificate that you are using, is in fact the one that you want somebody, that you want the people to be using and there is a way that we can add another layer of trust on top of that using DNSSEC. So we are starting to see some real business drivers where it is something more that you can say here is a very real and valid reason why you can go and do this, so that's part of it and beyond that we, with the people up here on the table and others, a number of us are all working on ways that we can help drive more demand for and more interest at it both at the CEO, CTO, CIO level, but also at the engineer level and provide more tutorials, more how-to's, more tools to go and do that. It's gotten a lot better, it's become a lot more simplified; I mentioned earlier you can just add a line to a config file and turn on DNSSEC. It didn't used to be that way, but you know this combination of things is all happening where it is becoming simpler, becoming more automated, and we are starting to be able to get the message out about why it is important in a much better way, the way it is coming.

RUSS MUNDY: I think that is a very good question is when we need to continue to ask ourselves and we have lots of people on this and involved with trying to help to generate with that honestly that's one of the reasons why we started this session to help people to try to understand why we are all want to go doing this. You can get the blue smoke and sorted out grey smoke and that's an important thing and if we keep working and explaining it in that manner for folks that don't really understand what DNSSEC is or how it works, I think that will help recognize it and it makes their internet activities more secure.

SPEAKER: I just want to mention too I think the Czech Republic has been the most successful of getting that option for us. You might want to chat with Andre, I assume he is here.

RUSS MUNDY: They are right here; SIDN is here and they are the folks that have done a great amount of work in the Netherlands, the folks who are from Sweden with dot se, if they are around here they have done a lot of great work on this too. So in those cases too if you look at what's happening, they have worked on both sides, especially in the Czech Republic and Sweden they have got a lot and Netherlands they have got a lot of ISPs doing validation and then they have also worked on increasing the signing.

JULIE HEDLUND: We do have a queue here. Please go ahead.

QUESTION: Hello, thank you very much. I am ____<72:41> from Fennec. My question is Fennec is now to apply to DNSSEC in the not very long future so what I want to you guys can give us some advice that we can make less error when we go and do DNSSEC in the early stage, maybe in the deployment process and system operation.

JACQUES LATOUR: I guess that something I can answer, so what you are talking is a variation to make sure that when you generate your own file you are 100% sure that its right at sero.ca, we spend a lot of time developing a solution around this and what we did is we did the lessons on all of these CCLTDs that run out first and made some mistakes here and there and I did find a pretty advanced functional specification on how we should do the DNSSEC to make sure it's right. Today there is a lot of signer technology, there is DNSSEC, there is different alternatives and what we came up with was and there is a fancy name for it, it's dual inline signer technology, so basically we signed the same zone with two different opening of the DNSSEC software and then we validate the output to make sure that neither one of the software that I don't really trust yet made an error, so if you just rely on one technology there is a chance that you are going to publish a bad zone, but if you validate in against two, the odds that you get the same bug with different software at the same time are very low. You can look at the torrent slide those are available on line, you can see the presentation there, pretty much choosy architecture of our solution, so basically we need to spend a lot of time on making sure of sign right and then you need to look at the validation so we do about 16 different tests after we generate the home file to make sure the signatures are valid, they are not expired, that no

records were deleted by mistake, we spend 6 months doing QA on those file generated and we found bugs in open DNSSEC that other people didn't discovered because of the way we were doing it, so we can talk offline if you want more details, but it's really important that you spend time on validating your output before you publish.

RUSS MUNDY: One of the thing I would suggest that Jacques didn't mention that may be in there too, the machinery that you are going to be using to do the validation of what is produced by your shining mechanism, you should also run some test zones against the validator that have intentionally known bad information to make sure your validator accurately identifies those failures. So, the first step would be to make sure the evaluators working right and you do that by throwing some data out that is known to be bad and there are several tools out there generating those and you know evaluators operating properly and then do that type of comparison. So rigorous testing I think is the message in planning for contingencies.

QUESTION: I am ____<76:43> from Yemen. I study and implement internet filtering circumvention technologies and one area that I was really interested was understanding how the detection of the headers of let's say traffic when it starts with the handshake, the headers are actually plain most of the time, so that is an area that I felt quite potentially vulnerability for DNSSEC itself, so haven't you considered for example encrypting the headers or the packages that are sent in order to maximize the potential for abusing the standards that are available, alongside of course the

certificates, something like DNS curve, some sort of protocol that has been introduced.

OLAF KOLKMAN: I used to be the Chair of the working group when DNSSEC got standardized and privacy, if that is what you are requesting, was a very specific non-requirement. We decided not to work on that because DNS data is public data, it was transmitted and clear for all of eternity at that point so to speak and it was a specific non-requirement to also privacy mechanisms to the protocol. The protocol only offers authenticity and integrity controls.

RUSS MUNDY: I think I will just add to that. There are technologies you can use to go and ensure the connection between the resolver and between the local system and the resolver. So there are ways to protect that last communication, that last connection, and we need to talk about that offline too.

DASHA VLADIMIR: Hello, my name is Dasha Vladimir from Russia. Just two questions about the implementation of dot ru. Maybe your impression on how successful it was, how long it was and how expensive it was, and it also says on the implementation map that now I am looking at the DNSSEC status for today and it shows that China is in experimental status and so what does it mean how long it will take them to implement? Can you compare these two?

RUSS MUNDY: I don't know the full history of China, but it's been in the experimental state for a long time because they have been working on different things, but on Wednesday you will hear a presentation very specifically about what their plans are. There is a slide, you can actually get it now, but there is a slide where they will be talking very specifically about their plans coming up and I think you can probably talk to the gentleman in front here bit more about that as far as what they are doing that. On the map itself the different gradations talk about the different stages that it goes through and it varies, into the points we made in the beginning a lot of the complexity and the time that's involved will change. Jacques talked about the months of QA and the work they did on that, others you know, apples and oranges it's very hard to compare just because of the size of the zone, the equipment that's there, the pieces, the policies and procedures, all of these, so we can't make an easy comparison around some of that because of what's there.

JACQUES LATOUR: It took us one year to sign dot CA and it took our DNS admin about 20 minutes to sign zero.ca.

DAN YORK: I don't know the specifics behind dot RU, I mean I know it has recently been signed.

RUSS MUNDY: I am familiar with the map and the collection methodology and so forth, I worked very closely with Chinkara on that project and the data that's collected is really all voluntary and people go to ask what stage would you put effort at and there is only general descriptive parameters, if you are doing this then you are probably here, and so the specifics of how long it takes anybody in a particular stage is completely up to the organization and as far as the actual collection of the information effort, they asked when you are going to be able to move to next stage, sometimes people say, sometimes people don't say, so like the example coming up with an apples and oranges even though it may have the same color on the map, they are really separate and independent and so it's really difficult to make any kind of quantitative comparison.

DAN YORK: With the exception that on that map once they are on the green thing that's when we can validate that we actually know that the records are in the root and they are being published so we can know that that is there. Can't give you a better answer around that, sorry.

QUESTION: My name is ____<82:44> from Palestine. I want to ask about the signature lifetime, how it can be measured?

DAN YORK: So you are asking about the lifetime of the signatures. Well inside each signature there is an expiration time that is in the signature itself and so we get back to the policy and recommendations. There is actually a document that was recently published that outlines some of these best

practices that are there and it varies. Many times people will publish, we are going to rapidly get down a rat hole to different kinds of keys and different kinds of things, but the key that uses to sign the zone data is typically maybe for a month or 3 months and there is another key that has been used to sign other parts of key that might go longer, to a year or so. It can vary. There is a document we can point you to that gets into the specific recommendation that have come about right now, it's called DNSSEC Operational Guidelines - Version 2, right now that's out there. It's an RFC 6781, will get you that information.

RUSS MUNDY: These are recommendations; they are not absolute requirements but a great place to start.

NICHOLAS: Hello my name is Nicholas, I am in the fellowship program as well. I am curious about the encryption algorithm you are using maybe for the handshake or for the different parts of the style, in other words discrete logarithm or factorization zone?

DAN YORK: We again descend into a deep dive but basically there are a numbers of different algorithms that are allowed in there, five of them or so, something on that line, but it is public key cryptography. It's a public key environment like that and there is number of them, I can't name them off the top of my head at the moment, there is a couple of the SHA variations, RSA, SHA1 and SHA3.

WARREN: And of course it is designed so that you can add additional protocols sector over time.

SPEAKER: And I heard you say Diffie-Hellman and I heard you say handshake; there is nothing like that.

DAN YORK: I wanted to clarify because it's really, I make a signature, I communicate what parameters I've been using to use that signature and I expect the client to validate that. There is no handshake, there is nothing like I can take these arguments and just give me what you have.

RUSS MUNDY: And part of the signatures, one of the fields in the signature record in DNS is the field for the algorithm used, so you specify it right in there so the validators can know exactly which algorithm it is. To Warren's point, there are people working on some elliptic curve cryptography and so they are looking at some of those and that would be yet another algorithm that will be added to that, so it's extensible.

THOMAS: I am Thomas, I am a German registrar, as for all public and private keys structures it's very important where the private key is stored and how safe it is stored, and I am very interested in who is in charge of the root key and the private root key and what will happen if this root key gets

compromised and if so is the whole DNSSEC resolving process broken at the moment and who is in charge of that?

RUSS MUNDY: Well there is a very substantial, well documented and well published approach that describes all of this there, ICANN is fundamentally the entity that is in charge of the root zone key signing key, but there are a large number of people from the community that have to be present whenever anything is done with respect to the route key, there is lots of hardware protections and physical protections, there is redundancy and is all well documented and you can actually go online and watch the archives of the key signing activity and Julie Hedlund has a role in the ICANN mechanisms that are all built to help make sure that the compromise does not occur.

SPEAKER: We can agree on that this is a very single point of carrier that could fail if that key is compromised that would be a big problem.

WARREN: So there is more concern at least some people that the key will accidentally destroy their compromise. Its two mixed up things, they have seismic things etc., but there is a lot of discussion underway now on how we roll the root key. There is a set of RFC, RFC-5011 is one of them, but this hasn't actually been tested yet and practiced so in theory you know a bunch of people get together and generate a new key and then you publish it and then one key signs the other key, but it hasn't actually been tested in the real world and so there is some effect on the

way, which I understand when people should try and enroll the key if they should rather wait until something really bad happened etc., etc, etc, and there is a huge amount of cross politics and policy around it. I think there is a discussion on root key.

DAN YORK: I was about to mention that there are two aspects, firstly the documents referred to if you go on and look to search online for DNSSEC policy and practice statement or DPS, those are the documents that exist out there and in most of the TLDs that have signed have also issued their own DPS, which states what exactly going on there, but the root one is out there very involved of the ICANNs DNSSEC, root.dnssec.org, whatever. There is a page has that all there. I would say anybody who is looking at one know how to sign CTLDs, go out and look at the DNSSEC practice statements because there are excellent documents that refer to exactly how different organization have gone and done that. On the consultation, ICANN does have a call for public comment and it in fact ends on this Friday, the final day of the comment and they are looking for feedback because this goes back to the best practices of today are that we have two different keys, there is a key signing key which signs the keys that are then used to sign the actual data and it is done that way so the key signing key can have a higher level of cryptographic protection etc. The root zone keys are being rolled every quarter and that is these key signing ceremonies that Russ is referring to, those are being changed all the time. But the ultimate key signing key at the heart of it all, ICANN has a contract that states it has to be rolled within the first 5 years and that's the ongoing discussion right now because it needs to be done before 2015 of the contract and

so ICANN wants to hear from you and they have put that consultation out there, you can get it off ICANNs website and they really want to hear.

JULIE HEDLUND: Just a little plug for Wednesday's session, so Joe from ICANN and Yab Ackerhaus from the Security and Stability Advisory will be talking about this issue. ISAC is actually also looking at the issue and thinking about what to say and so they will be joining into the discussion. It should be an interesting one. So I urge you if you are interested to come and hear it. And we are about a few minutes after the end of session so is there anyone else who has a last question before we roll this up? Then over to you Russ.

RUSS MUNDY: Well I want to thank everybody. Great set of questions today, great interaction. Thank you people, and if you have more and you are hungry for more information about DNSSEC, Wednesday morning we start at 8:30, earlier than most sessions because we have a big long day, so come join us Wednesday if you have any further questions or interactions.

JULIE HEDLUND: Thank you everyone, and there is lunch on Wednesday but you have to actually come and participate in the session.

[END OF TRANSCRIPT]