TORONTO – DNSSEC for Everybody: A Beginner’s Guide
Monday, October 15, 2012 – 17:15 to 18:30
ICANN - Toronto, Canada

JULIE HEDLUND: Thank you everyone. We will be starting momentarily. This is the *DNSSEC for Everybody Workshop* and please come in; we have space up here at the table. Please come join us. Don't be shy. Come, come, and we'll start just in a few minutes.

Welcome everyone. We're going to go ahead and get started. My name is Julie Hedlund and this the *DNSSEC for Everybody Workshop*. Please come take a seat. We've got a few more seats up here at the table. And without further adieu I'm going to turn things over to Simon McCalla from Nominet UK. And we do have handouts here, so you follow along with those and on the screen. Thank you.

SIMON MCCALLA: Thank you Julie. Welcome everybody. Thank you very much for coming along and filling the room and keeping us from being lonely here. So this session's all about understanding DNSSEC. And when I joined this community three years ago, I don't know about everybody else, but I found DNSSEC really complicated to understand. And it took me some time to work out how it all works; I'm not a DNS expert.

And one of the things we said when we were going to do a DNSSEC workshop was, wouldn't it be really nice to have a session where we just talk about the nuts and bolts of DNSSEC in kind of terms that are for the layman, not for the techie? And we try and find a way of talking about

DNSSEC which everyone can understand and take back to their businesses.

And so this is why DNSSEC is important for us, or for our registrar, or for our ISP, and so on. And so that's the purpose of this session. It's hopefully a really lighthearted session; hopefully it's really fun. We do some stuff that's a bit stupid and that's all part of the session. Please do interrupt. Please stop us. Please ask questions. Please come and stand up and take part if you'd like to.

There's a little handout here, which we give for the session. It explains who the speakers are and a little bit about the session, what we're going to do. On the back of this, if you've got the right printout, there are some really, really useful resources about DNSSEC. So if after the session you've got loads of questions that we can't answer, but you want to go and have a look then please do refer to these resources at the back. There are tools, and technologies, and libraries of documents and so forth.

We're really lucky, really blessed to have a fantastic panel of people here today. Just to introduce you to the panel of folks we've got, we have over here Roy Arends, who works for me at Nominet, which is great. Sitting next to him is Joao Damas, who is from ISC. ISC as many of you probably know have written BIND and are also real pioneers in DNSSEC.

We have Russ Mundy, who's from Cobham and from SPARTA. Russ has an enormous website full of DNSSEC tools and is part of the DNSSEC deployment working group. And last but not least, we have Matt Larson here. Matt works for VeriSign and has been very much a part of the protocol development of DNSSEC.

[background conversation]

SIMON MCCALLA: And we have a few other people taking part later on. We also have… Yes, exactly — just put it. Jay Daley, who is from .nz and he'll be being involved very shortly in the session. Without further adieu, let's kick off.

Many of you will probably have heard a little bit about where DNSSEC came from, you think it comes out of the IETF and all that good stuff. We'll that's absolutely nonsense. DNSSEC was invented about 7,000 years ago, as you can see. So we're going to present you the alternate history of DNSSEC. I want to introduce you to Ugwina, she lives in a cave on the edge of the Grand Canyon — she's an attractive lass. And then on the other side of the Grand Canyon is a guy called Og; he also lives in a cave. He's a good looking fellow.

And these two have got a bit of a thing going. The problem is between them is the Grand Canyon. It's a long way down and it's an awfully long way around, as you can see. So they don't really get to talk very much. But eventually on one of their kind of rare visits they sit around the campfire and they're staring into the fire and into each other's eyes and they notice the smoke rising up and billowing and they start to have an idea.

Once she gets back to the cave and when he gets back to his, they sit there and they communicate using smoke signals. And life is pretty good until this man moves in next door; a guy called Kaminsky. Now the problem with Kaminsky, he's a pretty mischievous fellow as those of you who've met him will know. And he kind of quite likes Ugwina, too, so he sets up a fire and starts sending her smoke signals.

Now the problem is poor old Ugwina, she's kind of getting all these very flattering messages over smoke signals and she hasn't got a clue who's who; she can't see clear enough and meanwhile Kaminsky's having all sorts of fun. So she says, "Alright, I've got to deal with this," so she sets off and she heads down the Grand Canyon, abseiling her way down to and visit and sort the mess out.

And they sit round and they talk to the wise village elders, and there's a chap called Diffie, caveman Diffie, and he's sitting there and he's like, "Mm, I might have an idea to solve this kind of love triangle out." So he jumps up and he runs into the back of Ug's cave because he knows what's in the back of the cave. And at the back of the cave is a big pile of blue sand. And the really clever thing about this cave is it's the only cave where anyone's ever found any of this blue sand.

So he's got a great idea. He grabs a handful of the sand and he runs out and throws it into the fire. And all of a sudden the smoke goes into this incredible blue color. And so now Ugwina is pretty sorted; she knows only to follow the smoke signals that are blue and not the ones that are gray. And life is good in the Grand Canyon again.

And that really is what DNSSEC is about. So if you take one message away from today, it's about that blue smoke, it's about turning the smoke blue so that you know you're getting the right response from the right person. And that's really all there is to DNSSEC. Now there's some really clever stuff in there and there are some clever algorithms; we'll talk a little bit more about that. But if you just get one message, if all you do is take that home and read some of the links on the back of that piece of paper, then hopefully you'll have learned something today, and hopefully it'll make some of that clear.

But I'll hand it over to someone who knows a bit more about DNSSEC than me and can explain a little bit more about how this all works.

ROY ARENDS: Thank you Simon. So I will get out of the slice and in front of you and I'm going to talk about DNSSEC. But before I can talk about DNSSEC, I of course need to talk about DNS. Now who has never heard about DNS before? Oh, that's good; I think we can rev up. Okay, and who understands DNS to a certain level in order to help us understand DNSSEC? Cool, so all of you guys who don't know this, ask him.

So I'm going to give you a small introduction to DNS. Next slide, please. So DNS is basically a hierarchy of names, of labels. An inverted tree, if you will, where the root is on the top — hence the inverted tree. And the root is on top and under that you have top level domains, like .uk, and .com, and .sn. Under that you have second level domains and so forth.

Next slide, please. The way you actually get to your destination as a client, the moment you type in a domain name, let's say bigbank.com and we will show you that in a minute, there is a result for somewhere that traverses the tree. It starts at the root, it goes to the next level, which is .com, and goes into the next level, etc., etc., until it gets the final answer of what is the address for this domain name.

It does some clever authorization as well. You can imagine that behind a very large ISP there are many, many folks going through, for instance, Facebook. And so that query only has to be [drove] once, because it's highly likely that that address for that domain doesn't really change that often, so a 'resolver' caches that information. Next slide, please.

[background conversation]

ROY ARENDS: Only seven times. Okay. So if you remember the slide that Simon showed you about a caveman, Ugwina here is basically the resolver. And Ug the guy on the right-hand side is the server. And of course in DNS, Ugwina is very, very liberal, it talks to many Ugs, to many servers. We're going to enact a little bit of a play here. If I can ask you guys to come up front?

So this is really the high level concept of DNS. I'm going to introduce you to a few folks. We've got Root over there, that's Simon on the right. And next to Simon is .com, who coincidentally is Matt Larson, who coincidentally works for VeriSign. Russ Mundy over here is bigbank.com and we have Joe User, who is today is Joao User, who will try to go to BigBank.com. And I am the ISP's Resolver.

So my good friend Joao over here wants to go to www.bigbank.com.

Joao User: "Please Sir, ISP connect me to my bank."

ISP: Perfect. I'm going to resolve www.bigbank.com; I have no idea where it is. I know where the Root is — right up there, so, I'm going to ask the Root.

ISP Resolver: "Can I please have the address for www.bigbank.com?"

Root: "Hi there, Mr. ISP. I'm afraid I can't give you the address to www.bigbank.com, but I do know where .com is, they're at 1.1.1.1."

ISP: Perfect, now I can go to .com at 1.1.1.1 and I'm going to ask him, "Where is the IP address of www.bigbank.com?"

.com: "Well, I don't know that IP address, but I can tell you that bigbank.com's IP address is 2.2.2.2."

Perfect. As you can see these guys are really good at delegating their issues. Next up we have bigbank.com.

ISP Resolver: "Bigbank.com at 2.2.2.2, could you tell me the address of www.bigbank.com?"

Bigbank.com: "I would be happy to. The address of www.bigbank.com is 2.2.2.3."

Perfect. So now I have the information for www.bigbank.com; it's at 2.2.2.3. I'll cache that information for later use. I cache all the information meanwhile that I've got from these guys, and now I can pass this information back to Joao User.

ISP Resolver: 'Joao, you want to go to 2.2.2.3."

Joao User: "I'm going there."

Perfect. Thanks guys. So this is really a high level of how DNS works. So there are a lot of people in your laptop trying to go places right now. Okay, next slide please.

So, when DNS was designed a very, very long time ago in internet terms, there was no concept of security. It wasn't needed. This protocol was basically designed by a group of people who tried to resolve a scaling issue. At that time they couldn't get host.txt files or host files fast enough around to cope with the ever growing growth of the then ARPANET. So DNS was basically designed with no security in mind; names are easily spoofed and caches are easily poisoned.

Let me just go into what spoofed and poisoned means. So spoofed means you basically pretend to be someone else. So for instance if you spoof a source address, you pretend to come from bigbank.com, but you're coming from elsewhere. Or you can basically tell folks that this domain doesn't resolve to 2.2.2.3, but to 6.6.6.6. We'll show you that in a minute.

What I mean with caches are easily spoofed — and this is really the bad part — a resolver that caches all that information has something called a 'time to live', that's in seconds. For instance bigbank.com could be cached for let's say about two days. That' means that if that's poisoned or spoofed, it means that folks who connect to this ISP's resolver are not going to go to the real bigbank.com, but to the fake site for over two days. So that's an issue we want to solve, and that's solved basically with DNSSEC.

So just to refer back to the slides Simon did, Ugwina, on the left, remember she's really, really, confused? She does not know who the real Ug is. It's very, very hard for the resolver to distinguish between two binary pieces of information when there's no assertion, things like cryptography and stuff. Thank you. Next slide.

So we are going to reenact the play, but now we're going to show you how spoofing is done in real life. Guys, can I have you up front again. So I'm not going to introduce you all again; we're just going to start off by Joao trying to go bigbank.com.

Joao User: "Mr. ISP, please, I need to check my account. Let me know where I have to connect it."

Perfect. Okay, www.bigbank.com; I don't have the information. I only know where the Root is, so I will just go to the Root Server.

ISP: "Root, address for www.bigbank.com?

Root: "I'm not really sure where it is, but I can tell you where .com is. And it's at 1.1.1.1."

ISP: "Thank you." 1.1.1.1. ".com, do you know the address www.bigbank.com?"

.com: "No, but I know that bigbank.com's name servers are at 2.2.2.2."

ISP: "Thank you. Hello, 2.2.2.2, I would love to have the address for www.bigbank.com. [sound of paper being passed] Perfect. Thank you." The address for www.bigbank.com is 6.6.6.6. I'm going to cache that information for future use and I'm very, very happy to connect my client to 6.6.6.6.

Joao User: "It looks like my bank; let me just go ahead and type my password in."

Perfect. Thanks guys. So this is how spoofing works in real life. Perfect. Next slide, please.

So the reason we are all here today is to learn something about DNSSEC and I'm going to give you a high level overview of DNSSEC. Now who understands a little bit of cryptography, like things with <Ps> and signatures? Okay, I see one raising his hand; I see a few. So again, if you need to know the details, go to these guys.

Digital signatures, what does that mean? Basically you have the concept of public key cryptography. Public key cryptography is basically you have a key set — it's a 'public' key, literally a key part that you can publish. You can put that on the internet and everyone can use it. And it's mathematically related, and excuse the term, it's mathematically related to something called the 'private key'. Literally you keep it private. You're not going to give it to anyone else. It's yours.

So what you can do now is you can send me information that needs to be private, so you can encrypt that with my public key. And only I can decrypt it with my private key. It works the other way around as well. I can now sign a piece of information and it doesn't matter what it is, and it's used all over the place and we're using it in DNSSEC as well.

You can now assign a piece of information with your private key; no one has that private key but you. And then you put a signature over that piece of data out there — just a piece of data — and now because other people have your public key, they can now assert that that information was really from you, because you've signed it with your private key.

So how does that relate to DNSSEC? Well, you know you can store anything you like in DNS. You can store addresses. You can store MX records. These things are used for sending mail. You can store text records. In fact you can even stream radio over DNS if you want to. So that means that you can also store a cryptographic key, a public key in DNS. And also the signature that you created over a piece of data; you can store that in DNS, too. So now, not only will you retrieve the address record for www.bigbank.com through DNS, you can also get the DNS key, you can also get the signatures. There's only a slight problem with that.

Next slide. Okay. From here on I'm just going to wing it. I promise you there are more slides. If you really want to look at them, they're somewhere on the ICANN website.

There is one issue with that because remember addresses and all this good stuff can be spoofed and of course DNS keys can be spoofed as well.

[background conversation]

ROY ARENDS: Perfect. Next slide please. So there's one issue, you have the address data in DNS, but remember that can be spoofed, and so can the DNS keys, and so can the signatures. So what you need to build is a chain of trust. And just like you have the root delegating to .com, delegating to bigbank.com — you can also have the root assert the DNS key for .com, who then asserts the DNS key for bigbank.com.

And this is what we call a chain of trust. And just like a resolver goes to root, goes to .com, goes to bigbank.com for the delegation pass, it can now trust www.bigbank.com because it's signed by bigbank.com, which key is signed by .com, which key is signed by root, which key the validator, which is me by the way, and the resolver has locally configured. Problem solved. We're going to show you that in the next play. Next slide, please. Thank you.

Guys can I have you over here again? I think I know where you want to go.

Joao User: "Please, Mr. ISP, connect me with bigbank and do a better job this time."

Perfect. Before I actually do this, I forgot that these guys need to be able to trust each other. And root of course, ICANN, and .com of course, VeriSign, they need to attach to each other's security. So this basically means that root is now able to trust .com, and .com does the same thing with bigbank.com; .com does now trust bigbank.com

Who know about PGP, how that works? Okay, Warren knows everything; Warren keeps raising his hand. So with PGP for instance, you have this chain of trust, this web of trust that people basically because A trusts B, B trust C, so A can trust C. It's basically implied trust. We have that here as well. Root trusts .com, .com trusts bigbank.com, I trust root, so I can now attest to all these things. Let's try this.

ISP: "Oh, yes, sorry, you want to go to bigbank.com."

Joao User: "I'm waiting for my answer."

ISP: "Perfect. I want to go to bigbank.com, what is the address of www.bigbank.com?"

Root: "Well, as you well know, I don't know that, but I do know where .com is, and that's at 1.1.1.1." I think that's enough ones. "And I'm going to sign that with a handshake."

ISP: "Perfect, thank you."

Since I have Root's public keys configured I can now check the signature that he just gave me — we do that with means of a handshake — but I now can trust this data, so I have a secure pass to .com.

ISP: ".com what is the address for www.bigbank.com?"

.com: "Well, I don't know that, but I know that bigbank.com's name server is at 2.2.2.2. Are we shaking or not?"

ISP: "Yes. Perfect."

Since I trusted Root's answer, Root sent me to .com, I can now trust .com's answer. .com sends me to bigbank.com.

ISP: "Hello bigbank.com, I would like to have the address for www.bigbank.com."

Bigbank.com: "That doesn't validate."

ISP: "I would like to have the address for www.bigbank.com.

Bigbank.com: "It is 2.2.2.3."

ISP: Perfect. Validated as you can see by this beautiful sign. This is now certified; I can store it in information. We've now defeated cache poisoning and here's the address for www.bigbank.com.

Joao User: "Thank you Mr. ISP. I like working with you and bigbank because you care about my security."

Perfect. So thank you guys. This is really how DNSSEC works. If you want to have more information, that little piece of paper in front of you has some references on the back, as Simon already explained. And now we're going to have Russ Mundy introduce you to some tools and some really, really cool stuff. If you really want to work with DNSSEC this is where you need to go. Russ?

RUSS MUNDY: Thank you, Roy.

ROY ARENDS: Any time.

RUSS MUNDY: Well, now that we know what DNSSEC is, and lots of people know what DNS is, we'll talk a little bit about how you can go about actually doing DNSSEC and implementing DNSSEC. So one of the important things that you need to consider when you're looking at doing DNSSEC is what does that mean for me, whether I'm a person, whether I'm an organization, whether I'm in the whole DNS realm and ecosystem, as is the popular term these days? Where do I fit?

So DNSSEC has many different places that it touches and so wherever you are in the DNS realm, the DNS ecosystem, it probably touches you in some manner. So if you're someone that holds names, just someone at the end that deals with the registrar. And you have a handful of names or hundreds of names, you will want to have the name servers of those zones for those names signed, and there's a set of things that you need to do for that.

If you're in a position of being a service provider for DNS activities, whether it's a registry or a registrar that does a lot of business, or a commercial name service operator and provider, you will want to different things, but you will want to be able to support DNSSEC as an extension of what you're currently doing in your business. Next, please.

So if you were a large business that deals predominantly in names, such as Registry Back-End, or someone who operates name servers for registrars around the world, and you may not be visible to the outside world, but you may be the people that are operating the name servers for a set of registrars Back-End providers, if you will. Then in that case you likely have a fairly knowledgeable and competent staff in DNS operations. And if you're going to add DNSSEC into that, then chances are you will want to work with that staff.

If you're an organization that's a major size, that's worldwide, that operates many, many zones as part of your business — HP is my example here — Hewlett Packard has been very active in providing their own DNS service for a long time. CNN is another one. They're probably going to similarly have a competent DNS staff that's integral to them. But many companies or businesses will outsource lots of things. And of course users, we all, make use of names, and there's a different set of things you do.

If you're www.verisign.com you probably will want to turn to the people that operate that to provide the knowledge the expertise to incorporate the DNSSEC things that you need to operate all of the names for that website in a signed manner. And in fact, I'm quite certain VeriSign has done exactly that to accomplish the signatures on their names.

Now, cnn.com and their website Money is one of their other delegations. They actually haven't gone through the process yet. I don't know if they have a back-end operator, I don't know if they operate it themselves, but in fact when you do a DNS lookup on the CNN homepage, there's over 100 DNS lookups.

Like you saw in our little skit here, because everyone of those little frames and little things that pops up usually has one, two, three, maybe even five or six actual name lookups that happen and so each and every one of those eventually does need to get signed. Now, over here HP is one of my favorite examples. They are an organization that's really big into names, so again they're organic staff. Next, please.

So the general principle that I'm talking about here is however you do DNS today, if you're a user and you essentially outsource all your DNS things to someone else, then that someone else is probably going to be the activity that you'll want to have do the DNS things. Whether you're a holder of names and you're buying it through a registrar who also happens to operate the name servers for those names, then that registrar you'll want to be the one that does the DNS signing of your names.

If you an organization that operates your own name server you'll probably want to do that yourself. If you're someone who is really into doing things yourself, you can operate your own DNSSEC. So for instance I'm kind of known as being into DNSSEC. There's DNSSEC that runs on this cell phone. So you don't have to have a big giant computer. It works, oh yeah, I saw some on my Android, so it can be anywhere, and you can do it yourself. That takes finding the tools. Looking through the starting points in the back of the paper gets you to a lot of what you need to do your DNSSEC whatever it may be. Next, please.

So for a single zone, what has to be touched? From the time that as a holder of a zone, you have your content of the zone, and it starts over here. You have your name servers, they're up there. You probably have a registrar of some sort in between, whether you're in a cc or whether you're in a gTLD.

And then running the bits on the wire on the internet are over here on the right hand side of the triangle. That's where all your name lookups and your resolutions, the things that talked about with cnn.com. You go there, you do a lot of name lookups and eventually your browser gets filled and each of those needs to get to the point where they're signed. Next, please.

So where you fit in the whole DNS architecture of things really then impacts what you have to do. If you're and end user you have to do one set of things. If you're a name server operator you're probably going to need to do a very different set of things. But it's necessary for everybody to do their part that so that it all comes together and DNS is available on a broader and growing basis.

Now the most important first question that almost anybody has to ask is who actually does operate my name servers? And it's a surprise how many people don't know that. So whether you're a consumer, whether you're the holder of a name, if you're doing resolution and you're in a home in the U.S., Comcast may be your provider. You may not know it, but you're already getting DNSSEC validation of all your name lookups. So as a home user in the U.S. with a Comcast provider they are providing your name service.

If you're a holder of names and you're being looked up, like DNSSEC-tools.org, it's signed, but we operate our own name servers and others do it differently. Next, please.

So what do you do? Right now if you're holding your own name, you put the zone data in, your authoritative name server and when somebody asks a question — like the resolver here in the bigbank.com, question — comes from a client, he asks it, answers come back and he gets it. And so really all you're doing… Can we have the next, please?

Oh, I thought I had my next one that shows… Okay, could we go back then one, Julie? All you're really doing is adding additional data that then the recursive server validates. That's what really DNSSEC is all about. Now it goes through a lot of different name servers, so there's lots of different places that it goes, and to fill the page — like I say, a hundred or so queries to fill a homepage. Next.

Another illustration of it, so that's just a map of how many DNS queries it took to fill that page, which was the CNN website about three years ago; it's bigger now. Next, please. That's what it is today; it got bigger. Next.

The important thing though to remember, it's the data in the zone that's the most important. The keys are important. They have to be safeguarded because they do validate the data, but it's the data that counts. The data is what matters; that's what's being protected. Next.

So what happens on the triangle picture, the data gets put in, it gets into the name servers and there has to be trustworthy things happen over here to get the data in. But DNSSEC works is out on the wire and you saw Dr. Evil jump in and give a false answer. This is where on the right hand side the DNSSEC applies.

So in general for what you're trying to do when you implement DNSSEC, if you're a user you want to do what you can to make use of DNSSEC and you'll do one set of things, like get some of the tools from DSNSEC tools or some of the things from NLnet Labs. There are a lot of tools out there available. VeriSign Labs has a bunch of tools. So as a user you can do a lot. If you're an enterprise, however you get your enterprise name service, you'll want to work with the providers and see if you can then get the signed data into the right places so that they are then getting your data to you for the users of your website in a signed way. Next.

So if you are operating your own — lots of open source tools, lots and lots of them out there. If you're using commercial products, go to your product vendor and ask them what I have to do to have DNSSEC applied to my names. Some product vendors have it already, some don't. If they don't, that's when it becomes a little bit harder because you can say, oh I either can't do security or I'm going to have to look at changing vendors, which is never easy, but it's always a possibility. Next.

So, if you're a service user, that's another question. So one of the services, if they aren't doing DNSSEC, ask them when they're going to provide it for you, or when it's going to be available. And if they aren't talking about when they're going to do it and won't give you any assurance of both the quality of the service and the DNSSEC availability, again, it's time to think about maybe getting service from somebody else.

Different outsource, if you don't have the expertise in-house, bring it in. It's available out there. If you already have people to do it, use your expertise today. So I'm going to turn it back now to Simon, and we're open for any questions that you might have from the play, or from the deployment aspects and various ways to do it.

SIMON MCCALLA: Thank you, Russ. So hopefully we took that journey from something simply to a little bit more complex towards the end. I hope that was useful, but I'd really be happy to take questions. We've got a huge panel of people here. We've got Warren, we've got Jay, and we've got a number of other folks in the audience, who I'm sure will be very happy to answer. Does anybody have any questions to kick off with? Sir, please use the microphone there. That would be great.

CHRIS TOUSSET: Thanks. My name's Chris [Tousset]. I was just wondering what would cost an average ISP to implement DNSSEC if they wanted to?

SIMON MCCALLA: Roy, do you want to take that?

ROY ARENDS: There are various costs in deploying DNSSEC. The root server operators have deployed this, the registries have deployed this, the registrars have deployed this. You're asking specifically about internet service providers and I assume by that you mean for instance, the Comcasts of the world. For them the cost of implementing is basically taking their current solution, which is probably something like BINDS or Nominum CNS, or Unbound and configure a set of keys.

Now that's the easy answer. The hard answer is what happens when stuff goes wrong? The DNSSEC makes DNS more secure, but it also means it makes it a little bit more brittle. And it's basically a binary thing, either the data is correct or not. Whereas DNS how it used to be, only some part of it had to be correct in order for you to go to a specific server.

So what you do not want to have of course is the moment somewhere else on the internet a DNSSEC signature expires. That means that people behind this ISP can't go to for instance facebook.com. And this actually happened with NASA.gov and Comcast. Where Comcast tried to resolve NASA.gov and couldn't get there because NASA.gov's signature was expiring. So a lot of people ended up calling Comcast, and blaming Comcast even.

So there are a few things you need to be mindful of as an ISP when you start deploying DNSSEC. Comcast as I said, have done this before. There are various other ISPs, I know a few in the UK, because that's where my company is based at, that have deployed DNSSEC. Some of them have literally just switched it on with no problem. And there are one or two of them who actually switched it off again because there was a problem.

So there are certain hidden costs involved as well, so I can't really give you a number, but I can give you an overview of a few pitfalls, and I think I just did that.

CHRIS TOUSSET: Thank you.

SIMON MCCALLA: Sure. Russ?

RUSS MUNDY: One thing that we have heard from folks that have done DNSSEC validation is that there are a couple of really important aspects that ISPs need to think about. One is training their service desk people, so that they understand what is going on at the time that they get some trouble reports, if there is something like the example Roy said.

But the other one is that it's part of an overall security offering — in other words, service providers that are looking to position themselves as our service to you the customer is better or stronger from a security perspective. It's not just DNSSEC, it's other offerings that are included in the security package, if you will, that's put forth by the provider. So it's more than just that my DNS is secure, it's that my ISP is offering a more secure capability to you the customers.

SIMON MCCALLA: Thanks Russ. There's one other thing as well, which is a bit of a minor plug, but a lot of registries and a lot of folk are offering DNSSEC signing services now. And they're recognizing that it's a little bit complex to deploy sometimes and there are costs involved if you got to train up staff and find extra service.

So VeriSign did it, at Nominet we do, and there are a number of other folk offer free signing services. So you can sign your domains and the bit that does the signing is handed over and then we pass back a signed zone. So those are free to use and if you want to speak to any of us about that then we can help out with that.

Anybody else, any other questions?

HUNAS KLAUSEN: Thank you. I'm [Hunas Klausen] from .D. Some years ago there was published a theme called "DNS Curve" as an alternative. How this one fits into the picture? It was told that it's cheaper and easier. Thank you.

SIMON MCCALLA: Joao.

JOAO DAMAS: Okay so DNS Curve addresses a different problem. DNS Curve is not designed to protect the data. During Russ's presentation you noticed that he was saying repeatedly that the important thing about DNS zone is the data, and that's the thing you want to protect. DNS curve, on the other hand, what it protects is the communication between one server and the next server.

When we were doing the skit, each of those interactions that Roy was doing, going back and for to servers, DNS curve would protect the communication between these two servers. But if any of them had data altered you'd still believe it. So you're not protecting the data, you're just protecting the transport; it's a different problem.

ROY ARENDS: I just want to add to that. With DNS curve we can now talk securely to Dr. Evil, to 666.

SIMON MCCALLA: Anybody else? Any other questions? Sir, please.

KLAUS HOLDERMOFFER: My name is [Klaus Holdermoffer]. I know it's very difficult to have exact number on that, but do you have any estimates or best guesses on how much of the internet currently supports DNSSEC? Or do you have any numbers how many of the let's say, top level domain registries actually support it, or even one layer below that? Are there any number available and how do you expect that to evolve in the future?

SIMON MCCALLA: So we can both answer that. Yes we do, we have some very accurate numbers, actually. And in fact on Wednesday the latest set will be published by the DNSSEC Workshop. There's a very significant portion of registries and TLDs that are now signed. There's also going to be in some of the presentations, some accurate numbers about how many domains are signed with DNSSEC as well. There've been some very big advances in that. I'm not going to give away those numbers, because that's part of somebody else's presentation, but do come on Wednesday and we'll have all those numbers for you.

RUSS MUNDY And there are some numbers now being put in place with respect to how much validation is being used out there. And that's an ever harder set of numbers to collect. But there are several folks that are working on those.

KLAUS HOLDERMOFFER: Another interesting number which is probably impossible to get is how much traffic actually is being supported by DNSSEC compared to the non DNSSEC traffic on the internet. Is there anything that you would have an idea how to get to these numbers?

SIMON MCCALLA: Roy?

ROY ARENDS: You're absolutely right, it's very, very hard to measure that and it also depends on your unit of measurement and the way you measure it. It also depends on which organization is measuring, I mean if you want to hash out the bias. I have seen some very interesting presentations yesterday during the DNSO session in combination the ccNSO Technical Workshop.

Duane Wessels from VeriSign showed us an interesting… I don't have the numbers ready, but I think it was about 4% of resolvers have switched it on. But 4% of a number of resolvers — it just needs to be one very popular resolver. That doesn't really cover the 4% if you know what I mean. So it's a very, very hard thing to measure.

Geoff Huston is the chief scientist for APNIC. Two weeks ago at RIPE gave a very, very interesting presentation about how he measures the amount resolvers validating. And how popular statistics, even broken down by country, and even broken down per country per capita, GDP and all that good stuff. His presentation is available if you go to www.potaroo.net and that has a lot of information. But that's all on the resolving side. And the rest of these measurements Simon explains.

SIMON MCCALLA: Thanks Roy.

SERGIO DEABRU: Hi, I'm Sergio [Deabru]. I just want to find out what is the increase on the load on the DNS servers because of this? I think I phrased that correctly. Obviously with the validation and everything else going on is there a huge increase in the load of the server?

SIMON MCCALLA: Russ you want to take that?

RUSS MUNDY: The load on the authoritative servers is a result of processing band width and memory. And Olaf Kolkma before he moved to NLnet Labs did a study when he was still at RIPE, I believe. And that's an excellent analysis and how you can use the same formulas. They seem to be very good holding over time to assess for authoritative name servers, the impact.

And the general conclusion was that an authoritative name server that has an expected growth rate that more or less is following industry norms should be able to do this, handle it with only — I think the numbers were on the order of 10%-ish or so, or less in all of the three measurements. So it is bigger, but it's a reasonable number and if you factor it in in your normal planning it should be no problem to handle it on the authoritative side. The recursive side is not as well documented. I think JPRS is trying to do some work in this area. I don't know offhand of studies that have been published. Does anybody else know of…?

JOAO DAMAS: I don't know published studies, but talking to the ISPs who have turned on validation, who are actually verifying that the information is correct, they have not observed a significant impact. Of course you have to realize that not everyone has plugged in DNSSEC at the same time, so the number of domains that you get to validate is a very small percentage of the total domains. So the actual practical input is small.

What every ISP has said so far is that they turn it on without worrying about resources.

SIMON MCCALLA: Something else I think it's probably fair to mention is there's quite a bit of talk at the moment about whether DNSSEC actually makes DNS amplification attacks worse, because of the amount of data that's traveling backwards and forwards. An amplification attack is where as soon as you send a DNS query out and spoof the name of where you want the response to go to. So it then bounces it on to another name server, then that bounces it on, and you get an amplification of the amount of data traveling.

And it's a good way of performing a DDoS, and of course with DNSSEC there's extra information traveling backwards and forwards. Now, I wonder if you just wanted to talk about that and the work that's being done around that?

MATT LARSON: Well, I mean you've described it pretty well. I don't know that I have a whole lot more to add, actually. It's something that if you run authoritative service with signed zones, you need to be mindful of, especially if you have a lot of band width and a lot of horsepower on your authoritative servers. This is something we're very mindful of at VeriSign for example because with .com and .net we've got servers with a lot of capacity and a lot of band width.

And so we need to be careful that people aren't using us as reflectors. That they aren't spoofing someone else's source address, sending a very small query, causing us to send a very large reply with signatures and a very big reply that would flood somebody else, attack somebody else. So it's possible to find large responses in unsigned zones, but DNSSEC just takes that problem and makes it little bit worse.

SIMON MCCALLA: Is there anything anybody else would like to know? We will be available to talk afterwards if you'd just like to come and ask a question off the microphone. We're very happy to do that. Is there anything else anyone would like to know publicly now?

Great. Okay, well we'll give you back the gift of time and end a little bit early, which I'm sure will be a relief for some of you. Thank you so much for coming. I hope it was useful. Please do come and grab us. There are plenty of resources. The presentations are available and there's also an audio transcript to this as well that's being made, as well as a video transcript, if you'd like to see that.

Again, I hope it's useful, and do come and ask us any questions. Thank you for coming.

[End of Transcript]