DUBLIN – DNSSEC for Everybody: A Beginner's Guide
Monday, October 19, 2015 – 17:30 to 19:00 IST
ICANN54 | Dublin, Ireland

DAN YORK: Hello? Hello? Okay. We just wanted to audio test this. Jacques, talk in this for a minute, I need to check audio levels on [inaudible] out there. I think you need to – okay, yeah. Could you bring that up? All right, Jacques, could you talk on this for a minute, I just want to do a little audio test.

[JACQUES]: The yellow fox jumped the fence. The brown fox jumped the fence. The [inaudible] fox. Hello, one, two, testing. Much easier in French.

DAN YORK: Good afternoon. Welcome. How's everybody doing on this first official day of the ICANN meeting? I guess there's been… The ICANN meeting start has kind of grown here, crept a little bit, but welcome. DNS security, DNSSEC. Let me ask a first question. How many of you here have deployed DNSSEC already? Okay. A couple of people. How many of you know how to spell DNSSEC? All right, a few more. Okay.

So we're going to give you a tutorial, series of things that we'll talk about, and you will get to see the Emmy award-winning – or no, I guess it's the Tonies. I don't know. Who's the theater? What's the theater awards? Tonies, okay. The Tony award-winning DNSSEC tutorial crew here. You can see them walking around with the white T-shirts. We have a skit, and yes, if you've watched engineers perform skits, here we are.

My name is Dan York, I'm part of the project here that's brought us all together. I work for the Internet Society, but I'm here as part of the DNSSEC Coordination Group, all the work that happens here. We have a whole workshop on Wednesday that will be six hours' worth of DNSSEC deep dives into different aspects around DNS and DNS security and pieces like that.

The one detail, I guess, I can't see here is I don't see the preview. Oh, but here's what we're going to talk about today. I'm going to give a little bit of an introduction about some basic concepts around this. We reviewed going to talk about some cavemen and blue smoke, pieces like this. And then we're going to get into talking a little bit more about what it is about, and then we're going to have our skit.

And then after we do our skit, Russ, who's standing over here with the big bank T-shirt is going to come in and go into a little

bit more detail around what we just witnessed, and then we're going to go through that from there. So let me begin.

In the beginning of our story here – and we should say, too, we do have remote attendees. This is going out in the Adobe Connect room. We're also streaming it live on YouTube for people who can't be here remote, and it will be recorded up on there, as well. So let's go back to 5,000 BC. Believe it, DNS and DNSSEC has been around since this very early days.

We have our friend here, Aguina. As it says, she lives in a cave on the edge of a canyon. And Og lives on the other side of the Grand Canyon, and Aguina and Og want to be able to talk, but it's a long, long way for them to go and do this, to go from one side to the other. They don't get to talk all that much.

On one of the visits, they decide that they could have smoke from Og's fire, and they say, "Hmm, maybe this could give us a way to send signals across the canyon. Now we don't have to go and scramble down to the other side to go and do this. We can just use these smoke signals."

So they're chatting away like this. Well then, one day, caveman Kaminsky moves in next door to Og, and he starts putting up his own smoke signals. All of a sudden, Aguina on the other side is confused. Which one of these is the one that she should be

looking at? Which is the right smoke that she should be doing? They're very confused, for their channel didn't work.

So she goes and decides to go across the canyon, back over to see Og, and find out what is it. And so Aguina and Og go to the wise village elder. Caveman Diffy says, "Hmm, I might have a way to do something here." So he jumps up and he runs into Og's cave, goes to the back of that cave, and he sees this pile of strangely colored sand. Now this sand only exists in Og's cave. So he says, "Hmm, bring some of that out and throw it into the fire. Now the fire turns blue." And all of a sudden, Aguina is now able to know which fire she should be able to listen to, which one she should watch because one of them has blue smoke and one of them does not.

And in essence, this is what we're trying to do is to provide you with blue smoke, trying to find a way to say, "This is the DNS entries that come from me, and I am the only one. My special sand says to all of you, 'This is my DNS info.'" And that's what DNSSEC is ultimately about is how do we go and do this?

So let's talk a little bit about what it is at the high level. We have DNS. We've seen this picture many, many different times. We have some kind of tree, and we'll have calm, big bank, UK, IE, SG, whatever. And we have this resolver that knows, that goes

out, trusts this hierarchy, it goes and sends this to the next level. We've seen these kind of pictures around of what goes on.

Challenge is just like when we had Og and that caveman Kaminsky. There's no way to know which of those signals, which of those answers is the correct one in and of itself. DNS works on speed, so whoever gets the quickest answer back to you is the one that the resolver will accept as the one that's there.

So it's this question of, hey, I could see that. That's the right one, right? So we want to bring out our team to do the first part. Are we going to break this into three parts and I'll do my other pieces? Or do we want to do all three at once? We already have this debate. We'll do it in three parts. So we'll do the first part first.

So here are our actors, and I'm going to get out of the way and let them do their piece. I'm going to turn it over to Norm, who is going to do the [leading] of things. All right. Here you go, Norm. And for the live stream, if you guys – yeah, because it's safe from where you are over to where Russ is would be cool. We've got our guy.

NORM RITCHIE: Okay. So what we're going to do is act out some DNS transaction with our incredible acting skills. And it's going to be a bit slower

than an actual DNS transaction, so what we have here, [inaudible] out here are various servers for the TLDs. We have root, com, and then a big bank, and the ISP. And I'm Joe user.

So Scene 1, Act 1. I'm going to do some banking, I'm going to pay some bills. I'd love to buy a beautiful, big TV like this I've been admiring. It's beautiful. So I'm going to do some banking. I'll sit down at my computer, and I'm going to type in www.bigbank.com.

UNIDENTIFIED MALE: Hello, Joe. Do you want to go to bigbank.com? But I don't know where bigbank.com. So I'm a recursive name server, I have no information, I need to go to the root, and ask the root. Hello, root? Do you know where www.bigbank.com is?

UNIDENTIFIED FEMALE: I'm sorry, I don't. But I do know where Com is. He's at 1.1.1.1.

UNIDENTIFIED MALE: Ooh, thank you! Hello, Dotcom. I want to go to www.bigbank.com. Do you know where that is?

UNIDENTIFIED MALE: Sorry. I can't help you, but bigbank.com is at 2.2.2.

UNIDENTIFIED MALE: Thank you. 2.2.2. Hello Big Bank, do you know where www.bigbank.com is?

UNIDENTIFIED MALE: As a matter of fact, I do. www.bigbank.com is at 2.2.2.3.

UNIDENTIFIED MALE: 2.2.2.3. All right. I got that. Doo, doo, doo, doo, doo. Hey, Joe. The IP address for www.bigbank.com is 2.2.2.3.

NORM RITCHIE: Oh, thank you, Mr. ISP. Now I can go off and happily do my banking at this address.

What the interesting here is that me, as Joe user, I ask my ISP to find me bigbank.com and everything else happened with the servers, and I just merely waited for the response.

DAN YORK: We just want to jump in here a little bit. So that was the first part. We had Aguina chatting with Og on the server. The server's confused. She doesn't know what's going on. So now we're going to go and figure out how to get that blue smoke and bring

that inside here and what it is. At the high level, again, we've got this concept that, as you saw, Dr. Evil was trying to insert – oh.

Well, we messed that up, didn't we? Okay. This is called what happens when you throw me into also trying to do a live stream at the same time. So now we're going to show you what happens when somebody tries to sabotage this. Okay. So I think we're act one, scene two.

Okay. So this time, we're going to do the same transaction now. We're going to do some more banking. Bills, bills, bills, bills, bills, bills. Another TV, bedroom. This time, we're going to show you what happened when there's a man-in-the-middle attack.

Okay. Well same scenario for me. Go to my computer, type in www.bigbank.com, Mr. ISP.

NORM RITCHIE: Thank you. You want to go to www.bigbank.com, but I don't know where that is. So I'll go ask the root. Hello, root. Do you know where www.bigbank.com?

UNIDENTIFIED FEMALE: I do not. You might want to ask Dotcom. He's at 1.1.1.1.

NORM RITCHIE: 1.1.1.1. Hello, Com. I want to go to www.bigbank.com, do you know where that is?

UNIDENTIFIED MALE: No, I do not. The name server for Big Bank, 2.2.2.2. Go ask them.

NORM RITCHIE: Thank you. All right. Big Bank, I want to go to www.bigbank.com, do you know where that is?

JAY DALEY: Yes, I do. You can find www.bigbank.com at 6.6.6.6.

NORM RITCHIE: 6.6.6.6. I'm going to remember that for a long time. Thank you. Joe, the IP address for bigbank.com is 6.6.6.6.

DAN YORK: Thank you, Mr. ISP. Now I've got to go off to this address and do my banking and get another TV.

Now we talk about what you saw there. So we saw them chatting. We saw that they don't know what's the issue route. So now the question is, how do we get that blue smoke? How do we do that? How do we bring this in here?

And so what we're going to see is that as Jay just did, as he came in as the attacker doing this kind of thing, something happened here. He was able to inject himself in there. So now we're going to talk about what goes on. What happens with DNSSEC is that in DNSSEC, there's a signature added. There's two parts, the signature added to the information that gets passed.

So when, as you saw, when Root and Big Bank and the Com name servers pass the information to the ISP, they provide DNS information and they also provide signatures. And these are the blue smoke, the thing that makes you unique to that particular piece. So they provide signatures.

Now the second part is that the ISP, Jacques in this case, is checking those signatures. What we call validation. They're validating the DNS signatures. These are the two parts that make it work. And each one of you could go back to your houses, your homes, whatever else, and you could turn on DNSSEC validation in your network or in your environment. Often, this is done by ISPs or it could be done on an enterprise network or a home network. You can do DNSSEC validation there.

The other part is you can sign your domains. They're two separate pieces of the puzzle. So we're going to look at that and see how this works. So the resolver, as we've said, checks these. It has what's called the chain of trust that goes all the way up to

the top of the root, this is the root public key, as we call it – this root that makes this whole chain of trust so that we know that the signatures are valid all the way from the root to Dotcom, to Big Bank, I see we're improvising some signatures right now.

We'll be able to go and show how this chain works. So what will happen, as you'll see, is that because there is this signature, and these signatures that go all the way down, this time Dr. Evil may have a few little problems getting in here. Let's come and watch this scenario here. Go on back.

First, we have to do a little exchange. So what's going to happen here is…

UNIDENTIFIED MALE: I am Big Bank and this is my signature.

UNIDENTIFIED MALE: Cool. Great to meet you. Hello, Root. I am Dotcom and this is what my signature looks like.

UNIDENTIFIED FEMALE: Hello, Dotcom. I am Root, and this what my signature looks like.

NORM RITCHIE: I'm the ISP, and I go the root signature here built in my software.

DAN YORK: Okay. Now everything is DNSSEC-enabled, everybody's signed their zones. Now we're going to do the same transaction again, more banking, got to get that TV. Lost it last time. Lost everything, actually. Okay. Same scenario. Get on my computer, do some banking. Mr. ISP, I'd like to go to www.bigbank.com.

NORM RITCHIE: Okay, Joe. You want to go to bigbank.com? Let's see where we go. Hello, Root. I want to go to www.bigbank.com. Do you know where that is?

UNIDENTIFIED FEMALE: No, but you can go to Dotcom at 2.2.2.2, but I need to sign this for you first.

NORM RITCHIE: Let me check. Okay. Everything's good. Thank you. Hello, Dotcom. I need to go to www.bigbank.com. Do you know where that is?

UNIDENTIFIED MALE: Wow. Bigbank.com is really popular. I don't actually know where they are, but you can ask the name servers. They're at 2.2.2.2, and here's the signature from me showing that that's correct.

NORM RITCHIE: Thank you. Now let me check, let me check, everything's good, good signature. Thank you. Hey, Big Bank. I want to go to www.bigbank.com. Do you know where that is?

JAY DALEY: I certainly do. Find it at www.bigbank.com, 6.6.6.

NORM RITCHIE: Let me check the signature. No signature. Hey! Not your bad knee. Sorry. Oh, that was bad. Okay, Big Bank. I want to go to www.bigbank.com, you know where that is?

UNIDENTIFIED MALE: Indeed, I do know where www.bigbank.com is. It's 2.2.2.3, and sure.

NORM RITCHIE: Oh, that's good. Signature has worked, everything is cool Thank you very much. Hey, Joe. I can guarantee the IP address is 2.2.2.3 for bigbank.com.

DAN YORK: Awesome. Thank you, Mr. ISP. Now with everything verified and validated, I can happily go off and do my banking, feel confident

that it's authentic. Let's have a good round of applause for the DNSSEC Players here, something like that.

So anyway, thank you, folks. We'll be nominating that for the Tony, Emmy, whatever that is, or something like that. So in all seriousness, if you do want to show other people this, it is now on YouTube. So anyway. That's a bit about what DNSSEC was.

So let me ask you a question. Do you feel better now? Do you understand a bit about what it's trying to do, the two parts to it? I'm seeing some saying yes, some people saying, "Eh," maybe no. Okay. So Russ is going to come up and talk a little bit more in a bit more detail about some of the parts of this. But remember again, the two parts. You had Jacques as the ISP, who was doing the checking, the validation. He was checking to make sure the signatures were there, and the other part was that the other people had gone and signed those signatures. That's what makes DNSSEC work.

And everybody who signs it has their own special keys, and they go and do that, and it's their special piece, their blue smoke, as we would say. It helps determine that that is their information. So I will pass it over to Russ to do further information, and here we go.

RUSS MUNDY: Okay. Thank you. I'll see if I can get the right direction here. Other one. Next. Okay. There. Hey, there we go. And I feel like I'm right in front of the screen. So maybe I was, maybe I wasn't. Anyway, I'm Russ Mundy and I've been involved in DNSSEC for quite a while. And we have discovered that we're really in a situation where you need to have some idea about why you need to do DNS security and what happens if you don't.

So the biggest single issue is that the names that you get out of the name servers, just like you saw on the last skit, can be wrong. And in the skit, talk about going to the banks or it could also be going through your search engine could be going to your stock management and stock watching here.

So anyplace that you go, almost anything you do on the Internet, you're going to be making use of DNS. And so when you think about what it is that your application is, whatever it might be, that's what people are going after when they try to attack DNS. Just like Joe User's case, where they wanted to steal his money out of the bank so he couldn't buy the TV. It could be intercepting mail, could be intercepting whatever.

So it really is not DNS itself. It really is what you're doing on the Internet that people, when they try to misdirect or hijack DNS are trying to get a hold of. At one point in time – and this has disappeared off the Internet, I am glad to say, but I did find a

course that was taught in a university about how to write software to hijack DNS. That was actually being taught in the course.

I looked through the syllabus that was up there was nothing that talked about ethics or that this was wrong. The professor was just using it as a nice, simple exercise in software development to do something a little bit "different." And so it really is not that complex and there is, in fact, a number of implementations for DNS hijack out there. So it's not really that hard.

So what is DNSSEC actually doing? Well you saw in the skit, it makes sure that the answer that the question – the answer that comes back to the question is the correct answer, it's the information that was put into the system, into the DNS system itself, by the holder of the information. In this case, it was the bigbank.com, so it was the information for how you get to www.bigbank.com.

So when the ISP goes through his validation process, he can tell that it came from the originator properly because he had the keychain that he followed and he started from the root trust anchor. And that also gives a validation of the technical correctness of the contents packet. So in security speak, it's source authenticity and integrity is what DNSSEC is doing for you.

So just a little [inaudible] here that is another way of illustrating what we were showing in the slide. When Joe User asked question of his ISP, it goes off to his recursive name server. The recursive name server asks the name server associated with the name, what's the name for it? It comes back, the recursive name server, the recursive name server hands it back to Joe User. And after all of this occurs, then Joe User can connect up to wherever he's going in our skit, www.bigbank.com.

So what happens when you get to the website and you see that you are getting DNSSEC validation? This is a specialized website that we've tailored because it's made to help [inaudible] DNSSEC to show whether or not you're using DNSSEC.

It's not a standard. This is just purely a convention. You see the little green DNSSEC check. There's a couple of other websites around that do it, but you don't normally see that green checkmark unless you're going to a site that's set up for it.

Now this is where you are using a browser that does not have DNSSEC validation by going to the same website. And so when you have the warning sign, it says, "Oh, my. Okay. You are not DNSSEC secured, so you don't know you actually got to the right place."

Let's put in Dr. Evil here in our picture again. So Joe User sends his query again, Dr. Evil is listening on the line, and you saw our

Dr. Evil, Jay Daley, doing a great illustration of how overlooking and eavesdropping and trying to get information at different places in different ways.

And in this case, Dr. Evil hears it and sends an answer back, and so the answer says, "Go over," – I should fix the number so they're the same, but the fake website instead of the real website. And although the query continues to go out across the Internet and come back, it doesn't matter to Joe User's computer because it previously got an answer, and it took that answer and used it. So proper answer, though it came back, effectively falls on the floor.

So when you include DNSSEC validation, what happens is validator says, "The answer that's coming back from Dr. Evil is wrong because it doesn't meet the requirement for the cryptographic check that is how we do DNSSEC." And it throws that answer on the floor, and when the proper answer gets back, then it can take that.

So in this case, these are some screenshots from an actual live demo that we did of a hijack in a meeting to make [point]. So you see those two screenshots. I know they're a little hard to read on this somewhat small screen. But in fact, if you look on the left side at the screen there, you see the top story is .org shares Comcast DNSSEC advice for ISPs.

You look on the screenshot on the right, you'll notice that's actually the second story on the page. Most webpages are made up of multiple links that have multiple names. So any one of those names can be hijacked, and in fact, that's exactly what we did in this case. And we inserted content. We didn't change content. We inserted content. The rest of the page [inaudible] so there's all kinds of interesting and different tricks that you can accomplish doing a DNS hijack.

And that [inaudible] that just came up are the number of queries that it [inaudible] homepage at CNN.com about seven years ago. That's about what it takes today, being bigger. What's really important and the stomp the foot professor point here is what matters about DNSSEC is the integrity and the content of the DNS data itself.

A lot of people think the most important part in a DNSSEC zone is the crypto keys and the DNSSEC associated stuff. It's not. It is all of equal importance, but if you want to rank anything, what's more important is the actual zone content data itself. Because that's what tells the rest of the software on the Internet where it's going to go. It's DNS content.

So here's another picture of a slightly different illustration, and how does one go about doing DNSSEC things? You've seen there's a lot of pieces of DNS and they're illustrated in a way

there. And on the right is the client and the recursive servers and center bottom authoritative [inaudible] top and the actual zone data that gets put in on the left side.

And so when you do DNSSEC, if you're the operator of an authoritative name server and you have zone data, then you sign that zone data. And if you're operating a recursive name server, then you get the root key and use that to turn on validation of data as it comes in from signed zones.

If you're a user, then you want to use some of the tools that are available, that are mostly free. If you support a user that has central support and you go to your central support and ask for it. So depending on the organization that an individual is in, there will be different kinds of things. Here it's an organization that's very DNS-centric and its main business line is DNS. You're probably going to have pretty competent DNS operation staff, or you will have outsourced it to a competent DNS operator.

If you're in another type of organization that just makes use of DNS as sort of I need DNS to work on the Internet, you might or might not have staff that's able to sort it.

So it really does vary depending on what the particulars of the situation are. So if you're, say, a registry that's responsible for a TLD operation, you better have pretty good DNS-qualified staff. Chances are they can do your DNSSEC already if you're in the

new gTLD. Something says it's going to [inaudible] here. I'm not sure what it is. Anyway, something is going to maybe go blank. I hope not. I'll talk fast.

So if you're an enterprise that is purely vendor-dependent, then at that point, you need to go to your vendor and ask your vendor, "I need DNSSEC. When can you [provide] it for me?" And the good old Internet end users, all of us, make use of as much DNSSEC as you can and ask, ask, ask. That's an important thing, because many times, when through the efforts getting DNSSEC out and in use, people will come back and then say, "But nobody is asking." So that's why in these sessions, I always urge folks to ask.

Protecting your zone data, that's really what you need to do. Keys and the crypto material provide that protection, but you need to also think about protecting your zone data if you're a zone operator and providing data for the Internet. That's really what counts.

So when you plug these pieces in, the simplest piece of getting a DNSSEC deployment in place and running is you've got some signed data from someone who's operating an authoritative zone, you've decided to do DNSSEC, you've signed your DNS zone content, and that ads the appropriate number of records and type of records into the zone. That zone data is loaded into

the authoritative server, and validating a recursive server has to get the root trust anchor, the root key – the root trust anchor is what it's called, but that's what you start from and go down through the tree, and you have DNSSEC going on.

Now depending upon where you're at, you may already have it and it's always great. You can ask your providers, "I really want to get DNSSEC. Am I getting DNSSEC?" And they'll come back and say, "Yes." But sometimes – in fact still, a lot of times – the answer is no. So that's why asking is so critical important.

But in terms of how you can impact your organizations and the type of organization you're in, because there are many different parts of DNS and DNS security. If you're in an organization that is highly centric on running a DNS activity as part of their [business], there's a good chance you can do these things that you need to do for DNSSEC in house. Not, if you're outsourcing them, whether it's for your operation or you're part of an enterprise, then you still need to ask the question, and whoever the service providers are, get them to give you a commitment about when they will be doing DNS security.

So that's the main set of things we wanted to present and talk about, and we're available for questions. There's a number of us here, and so we can take whatever questions you might have and this is what we like to get. People say, "Hey, what about?"

And, oh, we're going to need to run a mic around. It looks like we don't have mics on the table. Oh, Cathy has one. Open for questions.

DAN YORK: Yes. Think of your questions because you've got to have some after all this, I'm sure. I can see faces back there that say, "What?" Oh, please do state your names for the record, etc. Thank you.

[DENNIS]: [Dennis] [inaudible]. I represent a small ISP based here in Ireland. What is involved generalized we to move from today's, say, non-DNSSEC to a DNSSEC? Is it a large CAPEX or hardware/software, etc.?

RUSS MUNDY: Most of the mainline production software that's used in ISPs for resolution already is DNSSEC [capable] – not 100% across the board. But depending on what the package is, it is often a matter of simply turning it on, but the important thing before you actually go through and turn it on is to go through a testing process and prepare support people because there are some other things that can occur in the end user [view] if something

fails. It might look a little different to the end user. One of the largest ISPs in the US, Comcast – and they may be the [larger]—

DAN YORK: They are the largest.

RUSS MUNDY: Yeah. They have universally fielded DNSSEC, both validation and signing their zones, and they went through an extensive training effort prior to actually turning it on.

DAN YORK: Yeah. The reality is most of the code, like you said, BIND, NSD, PowerDNS, whatever you're using for actually for resolution. If you're using whatever it may be, Unbound. All of those, it's often just either uncommenting a configuration or putting [inaudible] in. They all support it. It's out there. Windows Server 2012, if you're using that. I mean, any of those kind of – the validation side is actually very easy to enable.

And so you can go back and immediately start doing that, and it doesn't really require much of a change or it doesn't have much of an increase on the capacity or the amount. I mean, there's additional checking it's doing, but it's not a [remarkable] amount for the typical ISP.

But the big change to what Russ was talking about. If Dr. Evil tries to get in there, what happens is there's a failure to get the information. Your validator can't get the information, and so it sends back to the other… I mean, what typically happens is it will send back to the user and say, "I can't get to that page."

The classic example is what happened with Comcast was NASA had signed their .gov domains, NASA.gov, because the U.S. Federal Government has been very strong in working with U.S. Government agencies such as that about 88% of all of the .gov domains are now signed.

But when you're signing a domain, there is some additional work that has to be done because every time you change, you update the domain, it has to be re-signed. There's also that private key – the thing that makes the blue smoke – that typically has an expiration period of about a year is the typical implementation that we do, and so a year after you sign it, you have to roll that key and have a new key.

Well, folks at NASA didn't do that right. They blew it. They didn't do the key rollover correctly, and so all of a sudden, their keys expired. What happened that made a perfect storm, that made this really bad was it was on – do you remember the day when everything was going to go dark on the Web for SOPA? Remember? There was that day when SOPA, PIPA, and there's

this protest, and Wikipedia was going dark, and everything was going dark and all that? Well NASA's keys expired on that same day. Okay?

And so all of a sudden, everybody who was using Comcast as their ISP couldn't get to NASA's website. And there wasn't an error message that said, "You can't get to NASA's website." It was like, "Server not found." Okay.

But, of course, people could go and whip out their cell phones, look at this, and their mobile network operators were not doing DNS validation. So they saw they could still get to NASA here, so what happened? "Comcast Blocking NASA" all over Twitter and everywhere else. It was this big, huge there, and they were like, "Wait, no, no, no. We're checking it."

So one thing from an ISP perspective is you may just need to train your tech support folks to know that if somebody calls up and says, "We can't get to NASA," or whatever, that one other failure condition could be that there's a failure in the DNSSEC validation.

And there's some very easy sites that let you go and you can just plug in NASA.gov and you can see, boom, boom, boom, bunch of green circles, red circles. Oh, hey, here's the problem. And so you could be able to go back to your customer and say, "Well, no.

We're protecting you from somebody putting bogus addresses in there."

But in this particular case, there was a configuration failure, and so there's [inaudible] with that. So that's the one thing that you need to be aware of as an ISP. Otherwise, you can start validating right now.

RUSS MUNDY: And one could go through a step-by-step process and test with a small group of users, and that sort of thing, too. But right, the validation end really is straightforward.

[DENNIS]: In the European market, could you give me any ideas what percentage of service providers are using it?

DAN YORK: Sure. It varies widely. We have some stats up on our Deploy360 page that go and show this. Some places like in Sweden and the Netherlands and the [Czech Republic], there's a very high percentage of ISPs who are doing it, very high. And I think Slovenia now, too, as well. And actually, Geoff Huston of APNIC does some statistics that he does that can show you on a country-by-country level of who's doing it. And so it varies.

In some of those, there's a lot because they've gotten together, they've worked on that. In other countries, there's almost very few. If Michele Neylon. were here, he'd probably tell me there's very few in Ireland who are [currently doing] it. There's two, somebody says. Awesome. Excellent. That was a better number than I was going to give, so that's awesome. Two ISPs. Build up more.

I see a gentleman. Okay. Thank you, Cathy.

RUSS MUNDY: The root name server is bringing you the mic.

UNIDENTIFIED MALE: All right, thank you. My name is [inaudible]. I want to ask an end user of the Internet, how would such person be concerned about DNSSEC? Because the techies could be careful when they're on the Web, but an end user who wants to go to bank.com, make some transaction, does not know what DNSSEC and security is all about on the Web. How could such [inaudible] because we need to talk to such people also [inaudible]. Thank you.

DAN YORK: Sure. So one of the challenges is with the end user… There's been one of these discussions. Should the end user even know?

Comcast has opted that the end users don't know, and that's the general thing. It's just there's a failure in that. Because one of the problems that's come up, and the reason why they don't, why the advocacy around this is how many of you look at that little lock in your Web browser? Okay.

How many of you ignore that when it goes yellow or do you even notice if it goes yellow? I see a couple of people. Anybody notice what happens when you get those warnings coming up about the TLS certificate? Do you actually pay attention to them or do you just click through?

How many people pay attention to them? All right. Good crowd here. It's probably why you're sitting here. How many people think that their parents, husbands, girlfriends, wives, somebody else out there who are not in this room, how many of you think they pay attention to those or how many think they click through them? Pay attention to them? Yeah, I'm not seeing hands. Okay.

So the debate is do we expose more to the end user? Do we give them more information like this? Because will the average user care? And the average user probably won't. And so it's almost a case of giving them too much information that they're not going to pay attention to. Oh, okay, so my lock's green or whatever else, or I have this other key.

For all of us in this room who want to look at this, there's some very cool things you can do. There are add-ons available from the CZ.NIC Lab folks that you can add on Chrome, Firefox, and IE, which I browse with, that can let me go and see if somebody has a valid DNSSEC signature, and it will give me a little green key in the browser bar.

For us, that's cool because we can do it and we can use it, and we can see it. For the average user, general feeling right now is it's one more thing they'll ignore, and so the effect really is to look at how do we do it at the network level, at the ISP level, at the enterprise edge, to just provide the protection as if it's just blocked?

Now there's a separate issue about how to educate some of those end users about why they might want to ask for DNSSEC validation, and why they might want to look at how they should get their domain signed. And that comes into this discussion we're sort of having here about what is the benefit of DNSSEC in increasing the trust in your domain name in your system, in your network, increasing the trust for your users that they can trust the information coming out of DNSSEC. That's kind of more of an advocacy discussion that needs to happen in the end user space. Does that answer your question? Anybody else? She's going in the back. Right?

UNIDENTIFIED MALE: Right here. Go ahead, Cathy.

UNIDENTIFIED MALE: Thank you. I'd just like to understand a bit more the difference between DNSSEC and the TLS/SSL certificate.

DAN YORK: Sure. So if you think about… They work together really well. Because I have a TLS certificate, what we used to call SSL, what that dose is it encrypts the connection between you and I, or the bank and you. DNS and DNSSEC has nothing to do with confidentiality. It doesn't encrypt at all. All it does is it says, "These are the IP addresses you were looking for." It says, "These are the right IP addresses that you got out. The information that you're getting out of DNS is the information that the operator put into DNS."

That's all DNSSEC does. So you know you're talking to the right place. Now once you talk to that right place, the TLS certificate that you get then provides a further assertion of who that person is, who that entity is, the server that you're talking to, and it encrypts the channel.

Now the challenge you get into is the two need to work together because you can buy a very fancy EV SSL certificate, you can get one that turns the whole address bar green. Okay. Whatever else. But if people don't get to your server to get that certificate, then they're not using it. Because they can get to this gentleman's server over here, who's actually the attacker, and he's bought a TLS certificate from somebody else who he was able to forge or get a domain name that looked similar to yours.

So you connect to his site, you get the little green lock up there because you've got a really good TLS certificate coming from him. You've got encrypted communication, you've got all of that, you're just talking to the wrong server.

So TLS and they work together – and are you about to say…

RUSS MUNDY: Yeah, the reason I put this slide back up is this is an attempt to illustrate how you can end up going to the wrong server, this is where the Dr. Evil jumped in, gave the incorrect address, and in this case, you go off to the attacker's website, but in the scenario Dan was just describing, the attacker has a certificate that will validate in your browser, either by trickery or because he bought a real, true, legitimate certificate, and you maybe typed the name a little bit wrong or something.

But it will give you a valid TLS/SSL connection to the wrong place.

DAN YORK: Now one way that people have looked at to fix this. How many people have heard of the DANE protocol? Anybody? [inaudible] there. So DANE is an exciting new usage of DNSSEC where it combines them. And what it does is it lets you put the TLS information into DNS and sign it with DNSSEC, and it can be either the actual TLS certificate you want to use or it can be the name of the certificate authority that issues the certificate or whatever else.

So now what happens is when you want to connect to your bank Web server, go to DNS, DNS gives you back the IP addresses, and the signatures validate those are them. It can also give you back a record that says, "And when you connect to that site, you should use this TLS certificate or you should use a TLS certificate signed by this certificate authority." One of those things. That information comes back to you.

You can now connect to the website because you've got the correct IP addresses, and when you get the TLS certificate coming back from them in the normal TLS handshake, you now have an additional way of validating it to know that that is indeed the correct TLS certificate that you want to use.

Wes Hardaker, who was here earlier, but he went to go somewhere else, but if you'll see him around here – and you'll see him on Wednesday – he's done a whole presentation on how this is being used with e-mail servers, and using it for TLS between e-mail servers, to be able to go and use DANE to know this is the TLS certificate that I want to use to connect to this particular e-mail server.

So DANE is this mechanism of combining TLS, the confidentiality and the pieces that you get, with the integrity checking you get out of DNSSEC so you can know what's there. And there's people implementing it in e-mail, in Jabber, in voice-over IP protocols. There's been some work on the Web side, there's some plugins that will do it.

The Web browsers, Google, Mozilla, and others have not yet bring this in. They have some of their own speed concerns and some other issues that they're still working through, and there's proposals in the IETF DANE Working Group. Warren Kumari, who was up here as one of the characters, he's one of the co-chairs of that group within the IETF, and they're working on how this could be used in more systems out there.

But that's what DANE is. DANE is using TLS with DNSSEC. Other questions. I saw somebody back there.

UNIDENTIFIED MALE: Good evening, [inaudible] from National Internet Exchange of India, NIXI. So my question is as I understand it, DNSSEC is not a foolproof solution because it just secures a connection from the ISP to the authoritative name serve, right? But what about if we talk about the [interim] security that is the connection from the [step] resolver to the ISP?

DAN YORK: So the validation, what you're saying about is the validation of where the validation occurs. The attacker could still get in and change the information. Right?

UNIDENTIFIED MALE: Yes. The connection from the [step] resolver to the recursor end resolver.

DAN YORK: So the reality is validation can occur at any point in the process, but depending upon where you do, there is still an attack surface for Dr. Evil to swoop in and give the wrong information. For instance, Google's public DNS servers, the 8.8.8 and the 8.4.4, as well as VeriSign's new public DNS servers that they've rolled out, both of those do full DNSSEC validation.

So everybody who's using the 8.8 etc., those are all doing DNSSEC validation right now. But the challenge is if you're sending your query, if your ISP is sending the – sorry, if your application, your Web browser, is sending the query out to the resolver and it's all the way out at Google's public DNS server, there's a lot of space that Dr. Evil could swoop in there and still get your information.

What we've seen is that's available, we're getting more and more ISPs who are doing it, so you're bringing the zone closer, then you're seeing people starting to put it into customer premise devices. So home routers and edge devices. Now you're moving that validation even closer.

I'm a DNSSEC geek, so I run a stub resolver, DNSSEC trigger. I run it on my laptop, but does the validation right there, and so now I further reduce where Dr. Evil could swoop in is that he would have to go and compromise my machine. And you've seen some applications that have built the DNSSEC validation right in.

If you see some of the VeriSign Labs guys running around, they've got an API called getdns, which includes the DNSSEC API or DNSSEC validation directly in that. The DNSSEC Tools Project that Russ is involved with has DNSSEC validation right there that you could build into your application. So it's not foolproof

because it does depend upon where does that validation happen.

RUSS MUNDY: And in general, the people have been involved in DNSSEC for a long time have pretty universally said that the closer you can get it to the software that's sitting in front of the user, the better. And there's even been some arguments amongst them is, "Oh, is it okay if it just runs on the general resolver, the stub resolver on the machine, or does it have to be built in to each application?"

That comes down to an argument of how secure the software on the machine is, but it gets to the machine, and there's pretty universal agreement in the DNSSEC world that, in the long term, that's where the validation is best done, on the end user's machine.

DAN YORK: And we're seeing, for instance, the latest release [inaudible] in the Linux world has DNSSEC validation turned on by default. So anybody who's using that on their servers or other pieces would have DNSSEC validation automatically on there. So at the device level. Other questions? I saw a gentleman up in front here, too.

RUSS MUNDY: I have a question over here. Yeah.

DAN YORK: Go ahead. Yeah.

UNIDENTIFIED MALE: Okay. You sort of answered it, but for the end user, the browser level, I've seen plugins for DNSSEC and then some seem native. Are there any recommendations on that?

DAN YORK: So right now on the browser side, it's plugins at this point in time. We've had long discussions with the browser vendors and the pieces like this, and one of their concerns right now has been they're all fighting on speed and on the speed of resolutions, speed of coming up with pages, and that additional checking does introduce a couple of microseconds. But this is the world in which they're working at.

Now there's some new work happening in the DNS working groups in the IETF that would pipeline some of those queries and do some other things, which look like they would go and help address some of the concerns that the browser vendors have around that.

So in the meantime, we're seeing a lot of pickup of DNSSEC in people using the plugins. We're also seeing a lot of it in other places, in the IM space, in VoIP, in SIP-related communications, in e-mail, in some of the e-mail work that's happening in there.

So it's happening in a lot of the other services that are happening out there, and I think that's part of it, too, is some of the browser vendors have said, "Well there's not enough signed domains so we're not going to implement this until there's a lot of signed domains."

And so what we're seeing is through some of the other pieces, we're seeing a rise of that. Now here in Europe, there's some great stories around that. There's over 2 million .nl domains that are all signed. There's a huge amount in some of the other different spaces that are out there that are doing that. So we're seeing a lot of the growth of that.

So we're still in… the reality is DNSSEC only really started to be useful five years ago when the root was signed. And so what we're seeing is now, over this last five years, we're seeing this growth path, and we're seeing the increase in growth in that.

UNIDENTIFIED MALE: Just a quick follow-on and related. So because I heard, it sounded like two possible contradictory points of view. So I

think I heard you say that there's one conversation about containing at network level or the ISP level. The other is bringing it all the way to [inaudible]. Is that just a process or is that a world view?

DAN YORK: I think it's an evolution. Because right now, we're seeing that the deployment is happening at the ISP level and at the public DNS level. We're seeing it out there. And then we're starting to see it happen at the edge of the network in operating systems and CPE devices, and we're seeing a few vendors putting it into their applications.

But as people become aware of what it can do, and as some of the vendors start to look and say, "Oh, I could do that with Dane. Wow, that's cool. Let me look at how to build that in." So we'll see more of that. It's an evolution. In the back?

UNIDENTIFIED MALE: The question is in two parts. Is there any good reason that an operator of a name server can give for not turning on validation of DNS requests? Second half then is there any good reason for an owner not to turn on DNSSEC or request their operator to sign?

DAN YORK: So the first answer is I would generally say there's very few reasons for somebody running recursive resolvers to not enable DNSSEC. The one caveat would be if they're not aware of the other error cases that can came up. Like we're saying, the failed validation could be cause of a failed configuration.

If the support staff isn't aware that this is something that could happen, then just somebody flicking, turning uncommenting a line in a config file and not cluing in the support staff may not be a good process point. But there's very few reasons why somebody wouldn't want to do that.

Some of the very large scale folks doing the resolvers, the amount, the bit of overhead that it costs to do that extra checking isn't a whole lot when you're at a typical ISP level. When you get to be a very large scale, and I don't know what quant it is, but there is some checking you need to do just in terms of capacity. For most folks, it's not an issue.

The second – Russ, would you agree with that?

RUSS MUNDY: Right. It's really not an issue on the validation side, primarily, if you take the support questions into consideration.

DAN YORK: Now on the signing side, it does get to be a little bit more complicated because there are a number… Like for me, I have my domains hosted across a number of different DNS hosting operators. A couple of those have made it very simple for me to sign my domain. I go in, I check a box, and I'm done. They take care of all of the signing of it, the regular… Because every time I update the records, they have to re-sign a zone.

They take care of rolling the keys for me every year. They do all of that. It's simple. In one case, I pay $30 a year to have a special added secure DNS service. In another case, it's part of the overall thing. So when the other DNS operators I use don't have any way of me doing that, I'm going to take it on myself if I'm an enterprise and I want to operate my own DNS authoritative servers, then I have to have the – I have to think about that extra process, signing the zone every time it gets changed, which most of the things like BIND or any of those not, etc. they go and they automatically do all that.

So the signing part is fine, but it is the key rollover every year when I'm rolling the primary key. Added process steps that I have to think about in there.

So that's the thing to think when you're going to sign your domain, the first step is does your DNS hosting operator – could be a registrar, it might not be, but whatever. Does the person

doing your authoritative name servers, is it easy for them? Do they offer the signing service?

If the answer is yes, and you can just check it, then boom, you're done. If they don't offer it, then you have to think, as in one of my cases, I had some domains with a registrar who is not supporting DNSSEC. I had to actually move them to a different registrar, eventually, to be able to – because I gave up on the registrar for providing any of the support.

So I had to move to that to do it. So you may not be able to work with that. And there are some TLDs do not allow DNSSEC yet at the top level.

We should explain. There's one more little piece of this. To make this web of trust work that we did here, the root, the .com domain had to be able to deal with signatures – .com does, so does .org, so does most of the original 22 that were there, and so do all the new gTLDs.

Many of the ccTLDs do, but there's about 100 that still do not yet, and we're slowly chipping away at those over the time, but there are some out there. So the ccTLD or the TLD has to support DNS at the top level, and then there one more piece that I don't want to really dive into, but I'll say the registrar has to be able to pass these records to the TLD. It's something called a DS record. Has to be supported in there.

RUSS MUNDY: So this is why we've tried to kind of abstract up what some of the pieces are because there are quite a few individual pieces, when you look at the entirety of DNS and what's involved. If, for the second part of your question, for an authoritative name server. In terms of size of operation, the largest TLDs by number of names are all signed.

We haven't looked to see how far down it goes, but I mean, clearly you have com, and that's by far and away the top of that pile and the other ones below them. One of the things that some of the smaller ccTLDs have given us feedback on is they just don't have the financial resources that they believe they need to incorporate the changes because they're running on really old, ancient stuff, and they just don't have the money to buy the new hardware that will run the newer, open source software that will support it. And that can happen.

DAN YORK: And as a result, you've seen some companies offering services to do that that kind of signing. I saw a gentleman – did that answer your two questions?

UNIDENTIFIED MALE: It did. Thank you.

DAN YORK: Okay. Gentleman in the back there with the blue shirt, in the teal shirt.

UNIDENTIFIED MALE: Most of the questions you have answered, my only concern is that [inaudible] DLS SSL could be compromised and some gentleman could take a very good equivalent of that and that could work, seem like that server. So can that happen with your DNSSEC? It could happen. If we want to take [inaudible] it could take the computer entity of the SSL as well as the DNSSEC, and then I don't have anything. Then you will propose me [inaudible] third.

DAN YORK: So there's two answers there. If somebody goes and they set up a name server, and they're going to say they're from ICANN.org, and they go set that up, they have a separate TLS server, they do something else, whatever else, they go and try to do that, they can even sign that record that they're serving out of their DNS server with a key.

But here's the point. There's what this chain of trust that goes from the authoritative name server for ICANN.org up to the .org registry, up to the root. And so ICANN has signed their domains, there is a hash of that signature that is now in the .org registry,

and is there. It's called this DS record that's out there, and that is then tied up to there.

So a DNSSEC validator would check all the way from the root down. So if somebody goes and tries to set up a separate server, separate DNS server, and serve our records and sign them, they can do all that. They can't get that signature, the hash of that, they can't get that up into the .org. So in a validation, when a DNSSEC, when a resolver that's validating checks that, it's going to say, "Wait a minute. You're giving me signed records. They don't validate all the way up to the root of DNS." Okay.

So they're going to check that. So that's the good case of where it works. Now the one got you is if somebody compromises your registrar, if they go in and hack your account on the registrar, and they go in there, then they can upload whatever records they want, and they can put in whatever records they want, and they can do that. That's separate from DNSSEC. That has nothing to do with DNSSEC. That's just regular DNS.

So DNSSEC, if everybody, if there's no compromise of the actors in the process there, DNSSEC prevents somebody else setting up a domain name in your name, and doing that. And that's what it prevents. But somebody else owning your name servers and taking over them, you've got bigger issues than DNSSEC at that point.

UNIDENTIFIED MALE: Another question is that in a chain, the weakest link [inaudible] strategy.

DAN YORK: I'm sorry. What?

UNIDENTIFIED MALE: When you have a chain, the weakest link, to have a weak link in a chain. But then maximum strength of that chain, that would break from there. Even from ISP, if it is not doing DNSSEC, then whole of the process is compromised. So you said that it is dependent on the ISPs. If one ISP in the world is not doing it, then all those customers who are connected to that ISP are not [inaudible].

DAN YORK: Correct. And this is one of the reasons why I was saying, ask your service provider for DNSSEC. Because no one can centrally dictate to people that they must do DNSSEC. The customers are key in where your describing.

UNIDENTIFIED MALE: In that case, the awareness of DNSSEC is the key [inaudible].

DAN YORK: Exactly. Hence why we're here, hence why we'll have the discussion that we're having on Wednesday, the efforts that we're doing. And also, we're starting to see that this become more of just best practices that ISPs should be doing, and as we're seeing more pickup and more usage of it, it's becoming something that customers are asking their ISPs and saying, "Hey, am I getting this additional protection?" And if not, can we go and do that? So it is that.

I think we've got time for one or two more questions. So something else, I see two more right here. Go ahead.

HORACIO: Hello, I'm Horacio. Your country domain name is DNSSEC, then your [inaudible] how secure is it? Because it won't validate up the chain.

DAN YORK: Correct. There's, at this point, if your country code, if your ccTLD is not yet signed, then what we would strongly suggest is that ICANN has a team of people who are standing by to help you sign your domain, and they will be glad to go out and do that. Seriously, Rick Lamb, who you'll meet if you come to Wednesday, but he's around here, as well. There's a team here

at ICANN that work with your ccTLD to do a workshop, to do the pieces, to get that signed, to help with the process in place to make that happen.

Because that's what you need to have in order for the subdomains to then get the added protection of DNSSEC.

HORACIO: Another quick question. How much overhead is being added on the request times in general when you enable DNSSEC? I mean, if your domain name, there's like gazillion [inaudible] requests. It kind of tends to maybe impact it.

DAN YORK: Yeah, and this is one of those. For the average ISP, for the average person, it's been generally small, it's been like under 10% in increase in the amount of bandwidth and things that you need to see. Some of those depend on the number of, Geoff Huston's done a number of presentations from APNIC around when you get into a large number of bad queries that can generate more traffic and more pieces around that.

So something to look at, the normal stats we've seen right now has been that for more ISPs, it's not a huge. I mean, it might be a 10% increase or [15%] increase in the number of the network

bandwidth for queries or something like that. But generally not a huge amount in the scope of things.

Obviously, when you get to be larger and larger scale, then you start to think about those kind of things.

RUSS MUNDY: Well, and there are techniques that you can use in terms of pre-deployment testing that you can actually set up a server that is doing validation, sitting right next to your existing production server that's not doing validation, and actually collect just feed a duplicate of the data into the one that's doing validation, and you can study and look yourself and see how much will it impact the performance of my machinery and my [plane].

DAN YORK: I think we have one more. I saw right there.

UNIDENTIFIED MALE: There's a computing, I think, I'm not sure whether it's a standard or not, but DNSCurve is there. That is based on [inaudible] cryptography. So is it complement to the DNSSEC or is it something different?

DAN YORK: So there's, what would you say, DNSCurve? Yeah, DNSCurve actually looks to solve a different problem, which is the encryption of the connection between the stub resolver and the recursor resolver. So it's really looking at how do you make sure that Joe, in talking to his ISP, how do you ensure that that connection is secure?

And that's one of the technologies that people are looking at to encrypt that last piece. There's also a working group within the IETF called Deprive, which is DNS privacy, which is currently looking at a mechanism, as well, that would use this, and DNS over TLS and some pieces between that. So it works on that.

Now one note that you did mention about elliptic curve. One of the things that we're seeing is that there is some concern about some of the cryptographic algorithms that are being used within DNS for the signing of keys, and the good news is DNSSEC was created from the beginning with the idea that the algorithms would evolve and would change.

And so for instance, a lot of the keys that are out there that are signed were signed with RSA-1024 crypto or RSA-2048. Well now, we're seeing a migration right now to using the elliptic curve ECDSA, which gives you a smaller signature, which to get to your point about the scaling of things. And one of the entities

[inaudible] Olafur Gudmundsson is with CloudFlare, and they're working, they're a large DNS provider [in the end].

They're looking at signing their domains and they're doing it with ECDSA so they can get smaller signatures, which can lend to more package and a more secure cryptography. There's some no crypto algorithms that are coming out of the Cryptographic Research Group that are looking at how do we feed those into DNSSEC, as well, so they can do it.

Now the challenge with that is that you've got to make sure that the resolvers can check those new signatures and got to have the signing software be able to sign it. So it takes a bit of time to roll those out, but there's definite interest in rolling elliptic curve crypto into the DNSSEC environment to do that.

Does that answer your question?

UNIDENTIFIED MALE: Yes. One more question.

DAN YORK: Sure.

UNIDENTIFIED MALE: Is DNSCurve and IETF standard? I'm not very sure about that.

DAN YORK: No, it's not. It's a product out of Dan Bernstein and some of the others who are involved with that project.

UNIDENTIFIED MALE: One last final question. If DNSSEC validation fails, some messages displayed in browser or what happens.

DAN YORK: So what it gives, when DNSSEC validation fails, it gives back what's called a serve fail in DNS speak, which means that the records are not found. There's nothing there. There's no thing. So what would happen in a browser [inaudible] it would say, "Server not found" or something like that.

And this is one, I was not involved when this was being standardized in DNSSEC, but there was apparently a good discussion about should it send back a different error message, not a serve fail, but DNSSEC validation failed. And that argument's actually been brought back in the DNS Operations Group within IETF to say, "Should we revisit that and come up with a separate error message?"

Because right now, well actually, it's options to the serve fail [inaudible] talk about it now. Because right now, you have now

clue. The server could have failed because it's really not there it could have been the authoritative servers failed or DNSSEC configuration fail.

So this has been, as DNSSEC has been more widely deployed, and people are doing this, this has been one of those parts of the feedback loop to say, "Hey, maybe we should do this a little differently." All right. Anymore? All right. One last one. And then we'll end this for here.

BASTIAAN GOSLINGS: Yeah, thank you very much for that. Bastiaan Goslings, amongst others, on behalf of Amsterdam Internet Exchange and ISOC Netherlands. My apologies in advance if I've not understood all the details, the technicalities of it. But I was wondering, imagine the ISP does a validation, we're speaking of a domain name, DNSSEC signed, but at the same time, the ISP is instructed by government to block at the DNS level that particular domain.

Besides the fact that you might argue whether that's the way to go, to try to block at the DNS level, but this is the fact that it's DNS signed, create anything additional.

RUSS MUNDY: I don't believe that would have any impact whatsoever. Whether the local jurisdiction and requirements are that you're operating

in, whatever the laws are there, you have to do the same thing. You [have to] follow those laws, and whether or not you had a name signed with DNSSEC or not, it really would not impact.

DAN YORK: The one thing it would do was that if you had a – if you were required to send back a bogus [record]. What you're saying in the blocking case, no. I mean, it would have no impact whatsoever because if you're blocking the DNS, you're blocking the DNS. So whether you get back a server fail, you get back whatever you're giving back.

But while you're there, I'll mention one last piece, which is to say that the ISOC chapter in the Netherlands, along with a bunch of other folks, put out a great site called Internet.nl, and if you just go there, Internet.nl, there is a Dutch version, but there's also an English version right there. It will test your – it will do two things. It will test the network you're on for whether it does DNSSEC validation and stuff, and it will also test the domain name.

So you can go there and test the domain name and find out whether it has the most accurate TLS, if there's DNSSEC sign and other stuff. So Internet.nl, a great site to go and check your domains. He wasn't a plant, really. No, but it's a good site that's there.

So with that, I think we'll draw to a close. Say thank you very much for coming here. We'll still be here for a few more minutes, and again, if you're interested in a lot more detail about DNSSEC, you can come to the DNSSEC workshop on Wednesday, starting at 9:00. It goes from 9:00 till 3:15. There's a whole series of different presentations. You can see the agenda online and we have it online. Right?

Okay. And it shows you some of them are bent as novice, some are intermediate, some are advanced. So you can sit there and know because we're going to have one, [beginning] of it is typically very useful because we have people from around Europe talking about what are they doing for DNSSEC deployment within their region or within their ccTLD or other pieces.

And then we're going to get into some pieces around some of the different applications that people are doing with DNSSEC, some of the different tools people are using, some of those might get a little bit more advanced in some of the ways they are. But do check it out. I'm not sure what room are we in?

RUSS MUNDY: Here. Right here.

DAN YORK: We're here. All right.

RUSS MUNDY: All day.

DAN YORK: Different configuration. All right. So we're going to be here. Come back up here. Come to the fourth floor for DNSSEC. And with that, thank you very much.

So just one other note, too. If you take that handout. On the back of the handout, there is a whole list of resources that you can use to find out more information. So there's different kinds of stuff on there, there's statistics, there's deployment maps, there's pieces around that. So lots of good stuff around there.

[END OF TRANSCRIPTION]