BUENOS AIRES – DNSSEC for Everybody; A Beginners Guide
Monday, June 22, 2015 – 17:00 to 18:30
ICANN – Buenos Aires, Argentina

DAN YORK: Good afternoon. Thank you for coming here to our DNSSEC for Everybody, A Beginners Guide. My name is Dan York. I'm going to be sort of MCing a bit of this today. We've got a session that has multiple parts to it. We're going to begin with a little bit of an introduction, that I'll be given, about DNS and DNSSEC and some pieces like that.

And then we have an esteemed cast of characters that are going to be coming up here to be part of a little skit that will dramatize DNS and DNSSEC and pieces like that as well. And then, after that, Russ Mundy will come up and talk a little bit more about some of the details. And then we're going to throw it open to a Q&A session.

In the past, what we've done is, the first part has only really gone about half an hour to 40 minutes or so, of the presentation, and then after that, we've had the remainder to be a Q&A time. So as you watch this, as you see this, as you watch the presentation, please feel free to think of what questions you would like to ask. We've got a great bunch of people, experts some of them, other people, pretenders, whatever.

All those who are here in the room to help us out. We do have remote participants. Julie, back over here, is interacting with the Adobe Connect room. So there will be some people there as well. When we do go to questions, and we'll have some microphones around, we will

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

ask you to say your name and affiliation, whatever you want to say, because that is going to be going out remotely to the people who are listening as well too.

This is all being recorded so, if you like the skit so much that you want to send it to your friends and relatives to go see it, they too can come and log into that. I'm giving this buildup here for… We'll see.

By the way, skit folks, I have to tell you, for the camera, we need to go from here to there. And we will also blank the projectors, but… There is a little key that you could push called B which blanks these. No, we don't want to use that. Anyway. Before we begin, I want to find out a little bit you all.

How many of you are here at ICANN for the first time? Okay, good. How many of you have done anything with DNSSEC? Actually, let me reverse it. How many of you have never done anything at all with DNSSEC? Okay. How many of you didn't even know how to spell it before this meeting? Okay, all right. Anybody… Okay. How many people have really done a lot with it? Okay, yeah, a number of people here who are in this space. Okay.

Actually, while we're just getting word out, what are some questions that some of you might have? If you just want to throw them out quickly, as far as things that you might like to know about? Why are you here? I should say.

UNKNOWN SPEAKER: Like what is DNSSEC?

DAN YORK: Yeah, what is DNSSEC? What is that here? And you know the things, why are you here? Just nothing else on the schedule worked? Right, okay, right. You heard there was a skit. Okay. So all right. Well, let's get going here. I'm going to begin with a little bit of an introduction. And to do this, we want to go back a little bit and get into sort of the beginning of DNSSEC and why this matters.

So we're going to dive back actually into 5,000 BC. And we're going to tell a little story here about [Aguina]. She lives in a cave on the side of the Grand Canyon, and she wants to go and, well here is [Og], he lives on the cave on the other side. And they would like to go and communicate. It's a long, long way. They don't get to see each other much.

So they're trying to figure out how to talk to each other more. Well, one of the visits that they are there, they notice that there is a fire coming from this, the smoke here from [Og's] fire. And they say, "Well, what if we do something with this?" So pretty soon, they start using smoke signals to communicate. Going from one side to the other.

And this all works great. They're having great conversations, they don't have to go all of that way. They're being able to communicate and do all of this. But then, one day, the mischievous caveman [inaudible] moves in right next door, and he starts sending smoke signals too.

All of the sudden, poor [Aguina] on the other side of the cave, on the other side of the canyon, can't figure out which smoke signal is really the one that she wants to watch.

So she goes off to try to go across the other side to figure out which of these is the one that she should pay attention to. She and [Og] go to the wise village elders. Caveman [Diffy] says, "Hmm. I've got an idea about this." So the elder, here, goes into the back of [Og's] cave, and he finds in there some strangely colored sand, that is in [Og's] cave, and only in [Og's] cave.

And he brings that out, and he puts it in the fire. The smoke turns blue. All of the sudden, [Aguina] is now able to figure out, which of the smoke signals is in fact the correct one that she should be paying attention to.

In a nutshell, that is what DNSSEC is about. At a fundamental level. It's about helping you know that you're getting to the correct, in this case, the correct set of smoke signals. So really what we're here talking about is, how to get you blue smoke, only in a little bit more complicated of a way, because it's not just quite that easy.

But we are going to talk about how you can do something so that somebody could differentiate between your address, your information, and that of an attacker could put in there. So, with that, we're going to talk a little bit about an introduction to DNSSEC.

So at a very high level, we're all familiar with this. We've got the root, we've got the top level domains, UK, COM, SG, AR, whichever ones we happen to have in that kind of space. And this is what the root is. We have on all of our systems, or in our own ISPs, we have a resolver somewhere. A resolver is a little piece of software that goes and helps translate those domain names into IP addresses.

Because ultimately, all of our computers and devices have to use IP addresses. And we don't care whether it is IPv4 or IPv6. It gives back the appropriate information that's there. But the resolver goes out and it makes these queries, and it keeps doing that until it comes back with the answer that the computer can use. This is how DNS basically works.

The challenge is with DNS in general, is that there is no security, in basic DNS. It's what, whoever gets the answer back quickest, is the one that you get. So if you're trying to get to NIC dot AR down here, or if you're trying to get to Google dot com, or get to your bank, or whatever it might be, you're going to that. You're going out and getting that information from DNS.

And what's happening is, DNS is just giving you whatever answer it gets back the quickest. It's what are called caches. Once your DNS resolver has an answer, it holds onto it for a certain period of time. Well that information could be poisoned, as we say, the attacker could put the wrong information in there. And that's what happens in here.

So we're now going to bring up our little team to go and do our skit. It's actually in a couple of different parts. So if you just want to hit that. There we go.

All right. Let's introduce our folks as they're coming up here. We have Warren [inaudible], Jacques [inaudible], Wes [inaudible], Russ Mundy, and Norm [inaudible] is going to be our MC and me… What? I don't know. Sorry. Norm.

NORM: Thank you. So we have our esteemed acting troupe here. What we're going to do is, these guys are DNS servers. I think you can see the resemblance. So what we're going to do is act out, and show you in slow motion, how a DNS transaction works.

So, I need that little piece of paper somewhere.

One second. We need our props.

There we go. Okay. So the scenario we have here is doing some banking. So I, as you can see, Joe User, I'm going to do some banking. And these are the… Where did my ISP go?

And I have my friendly ISP here. So I'm going to start off, do some banking, pay some bills. I'm going to type in the address I want to go to, which is www Big Bank dot com. I hand it off to my ISP.

UNKNOWN SPEAKER: Hi. So you want to know where www Big Bank dot com is? I don't know. Hold on a sec. I'll get you the answer.

And I will start at the right place. Excuse me, Mr. Root? The top of the DNS tree, I got this whole long question. Where is www dot Big Bank dot com?

UNKNOWN SPEAKER: Huh. Sorry, I don't know where that is. You should go and ask dot com. He's at 1.1.1.1.

UNKNOWN SPEAKER: Got you. Follow the street down to 1.1.1.1.1. Excuse me, do you know where www dot Big Bank dot com is?

UNKNOWN SPEAKER: Hmmm. I don't know where www dot Big Bank dot com is. But I know where Big Bank dot com is. There are at 1.2.2.2.2.

No. 2.2.2.2.2.

UNKNOWN SPEAKER: You started that part two early. Hello Mr. Big Bank. You're the DNS server for Big Bank dot com, so I'm really hoping you'll know where www dot Big Bank dot com is.

UNKNOWN SPEAKER: Well, as a matter of fact I do. www dot Big Bank dot com is at 2.2.2.3.

UNKNOWN SPEAKER: Awesome. I will go tell the user immediately.

User, you need to go to 2.2.2.3 to talk to www dot Big Bank dot com.

UNKNOWN SPEAKER: Thank you Mr. ISP. Now, me and my laptop can go off to 2.2.2.2.3, and do our banking, which we then connect to the bank. And away we go.

So that is the DNS transaction.

UNKNOWN SPEAKER: There is more to come, you've seen nothing yet.

DAN YORK: So this is the transaction happening, you know, millions of times a second even higher than that, these incredibly high rates, every time that you're going to every single DNS domain name. Every time you're doing that, this transaction is happening. Now we talk about caching, the reality is that Wes has that answer. He would hold on to that and give it back to people for a certain period of time.

So he's not asking this whole process every time, but this process is what's going on. Any questions about this, before we show the attacks and what can happen? Questions right now? Okay this is basic DNS. Now we're going to get into a scenario, where we're going to show what can happen when something else goes on.

Oh, you've got another mic, okay.

UNKNOWN SPEAKER: We're doing good. Okay. So act two. This time, we're going to do some banking, and this time, there is going to be a man in the middle attack. So we'll do some more things.

UNKNOWN SPEAKER: Yes sir, yes sir, right here.

UNKNOWN SPEAKER: Okay. So more bank, more bills to pay. Bills, bills, bills. Off I go again. So I type in www Big Bank dot com. And that goes off to Mr. ISP.

UNKNOWN SPEAKER: Got you. I'll go look it up again, because I've already flushed my cache for the day. Mr. Root, can you tell me where www dot Big Bank dot com is?

UNKNOWN SPEAKER: Sorry no. But I can tell you where dot com is. Dot com is at 1.1.1.1.1. Go and ask him.

UNKNOWN SPEAKER: All right. I guess that will do for now. Dot com, maybe you're smarter, can you tell me where www dot Big Bank dot com is?

UNKNOWN SPEAKER: You want me to answer that? No, I don't know where www dot Big Bank dot com is, but I know where Big Bank dot com is. They're at 2.2.2.2.

UNKNOWN SPEAKER: Well, I'm narrowing it down. That's good. Mr. Big Bank, do you know where www dot Big Bank dot com is?

UNKNOWN SPEAKER: I certainly do. You can find it at 6.6.6.6.

UNKNOWN SPEAKER: Awesome. I will go tell my user, loser, right away. Here you go, Mr. User, I have got the answer for you. It's at 6.6.6.6. Please go make lots of deposits.

UNKNOWN SPEAKER: Thank you Mr. ISP. Now I can happily go off and do my banking with Big Bank at 6.6.6.6.6.

So.

DAN YORK: All right. So let's give our team a round of applause for this second act.

So this is the attack. Now we've got one more part to this, all right? But this is the attack you saw. And you saw here that Dr. Evil swooped in, in front of the correct authoritative resolver, because he was able to get there quicker.

Now it could have been, he could have done something to go and do a denial of service attack, or something, against this root server so it wasn't available. And so only he was there. Or it could have been that he was in, he was able to get to the point in the network where he could answer the ISP faster. There is a couple of different reasons how this attack could take place.

But the net of it was, that Dr. Evil here, the attacker was able to get into the place, and get the answer back before that. Now, the ISP, the resolver, said, "Oh great. I got an answer." That's all the ISP wants, or the resolver. All the resolver wants is an answer. It will take whatever answer it gets, the quickest it can, and get it back to the user.

So the resolver was perfectly happy, because it was not doing any kind of checking, it was not doing anything. It was just taking whatever answer it got, and brought it back to the user. That's how DNS works. And that's how the attacks can happen. That's how what we're calling here cache poisoning and other things are there.

So any quick questions about that before we show the DNSSEC answer here? No. Okay. Well now we're going to do this again, act three, with… Oh, we need one more little piece of paper here.

UNKNOWN SPEAKER: Going to do signing first.

DAN YORK: There is another step that happens in here that all of these folks have to do, to make sure that they all agree.

UNKNOWN SPEAKER: Okay. So this is act three. So enter DNSSEC.

UNKNOWN SPEAKER: Hello. So I'm the root. You say you're dot com, are you sure you're dot com?

UNKNOWN SPEAKER: Yes, I'm sure I'm dot com.

UNKNOWN SPEAKER: Okay.

UNKNOWN SPEAKER: Hi, I'm dot com. Big Bank, are you sure I'm dot com? Are you sure you're you?

UNKNOWN SPEAKER: Well, in fact, we have gone through a set of steps that are defined by procedures that says, yes, I know I'm me. I know you're you, and we've exchanged credentials.

UNKNOWN SPEAKER: Great. So I know who I am.

UNKNOWN SPEAKER: All right. Mr. Root, I am an ISP. I need to verify who you are at the beginning of all of this, and I'm going to memorize you from now on to make sure that this handshake is 100% real. Thanks.

UNKNOWN SPEAKER: There we go. That was DNSSEC signing. Interesting to note, me as the user didn't do anything. I don't have to worry about anything else, other than I want to do some more banking.

So more bills to pay, more banking, this time with DNSSEC. Start off, www dot Big Bank dot com, type it in, and hand it to Mr. ISP, please.

UNKNOWN SPEAKER: Got it. I will run right away and answer that question for you. My dude, I'm from California, wants to know where www dot Big Bank dot com is. Can you tell me Mr. Root?

UNKNOWN SPEAKER: Sorry I cannot. But I know that dot com is at 2.2.2.2, and let me quickly sign that answer for you.

There you go.

UNKNOWN SPEAKER: Thank you very much. And I've checked the signature, and I know that it's valid. So now I'm going to go to Big Bank dot com, and I'm going to ask you, where is www dot Big Bank dot com please?

UNKNOWN SPEAKER: I don't know where www dot Big Bank dot com is, but I know where Big Bank dot com is. They're at 2.2.2.2, and let me sign this.

UNKNOWN SPEAKER: Yup. That signature matches. Okay, off to Big Bank. Hello Mr. Big Bank. I'm looking for www dot Big Bank dot com. Will you please tell me where it is?

UNKNOWN SPEAKER: Certainly I will. It's 6.6.6.6, really.

UNKNOWN SPEAKER: No, no, no it's not, because you didn't sign it. And if you did sign it, you didn't sign it appropriately. So I'm going to ask again. Do you know where www dot Big Bank dot com is? And hopefully I'll get the right server this time.

UNKNOWN SPEAKER: Well, I am Big Bank dot com server, and www dot Big Bank dot com is at 2.2.2.2.3, and I will sign it. There you go.

UNKNOWN SPEAKER: Yup, and that signature checks out. So this is my definite answer for you Mr. Joe User. Here is your signed and gold starred answer.

UNKNOWN SPEAKER: Wow. Thank you Mr. ISP. Now I can confidently go off to 2.2.2.3, and know that it has been authenticated throughout the chain of DNS queries. And that is how it works.

DAN YORK: All right. Well, just a couple of notes as the folks are going back there. Notice that that there is two parts to DNSSEC. One is that the resolver had to do the checking. So in this case, Wes is the ISP, and the note. We talked about this as being at the ISP, and for a lot of people, that's typically where it is.

Your DNS resolvers, when you are, when you're on a network, you are typically at a, at your ISP. They're not always. They could be, if you're inside of a corporate network, they might be at the edge of your corporate network. You know, or it could be some of us here, are running them on our own laptops, because we're DNSSEC geeks who do that kind of thing.

Okay, they could be in your home network, for instance, they might be on your home Wi-Fi router, might be running a DNSSEC validating resolver, or a DNS resolver there. It might be somewhere else in there. It doesn't have to be in your ISP, but in this example we're doing that because of that. So one side is the validation, which is checking to make sure that the signatures are correct.

And that's actually something that all of us can do, is to go, when you go back to our office environments, or to our home environments, we can look and find out, can we enable DNSSEC validation? Is it something that we can turn on? If you're in a corporate environment, if your ISP supports it, you'll be able to go and use that.

And in some parts of Latin America, it's already turned on for ISPs, and in some parts of Europe, and in some parts of North America, and other areas. In other places, it's sometimes just a change of a line in a code file, that configuration file that needs to go and turn it on. But validation, the checking, is the one part. And in the other part, is what the other root servers did to go and create these signatures.

There is a signing of the domain that happened, that Russ is going to get up and talk about in a moment here, but the signing that happened in this case, at Big Bank dot com, they signed their zone, they sign, they put a cryptographic signature on there. They did that, and then there is this chain of trust that verifies it through this whole process.

So signing and validation, two different parts to DNSSEC. So I'm going to turn this over to Russ, and let Russ talk a bit about what we're doing in here. I think we're going to do it, right?

RUSS MUNDY: Okay. Thanks Dan. As we have a set of information here, and there is actually a lot of words on these slides, but I'm going to intentionally, go through them very quickly, because we really want to save a substantial time at the end for questions and answers.

So if I zoom by anything too fast at the time, you can stop me then, but it's probably kind of better to jot down your question and we'll try to collect them all at the end, because sometimes we get better interaction between folks from building one question to another.

So, we have already talked some about why do you worry about somebody hijacking DNS anyway. The example in the last one was that somebody wanted to get in the middle and steal some bank transactions. Clearly something of interest to people that want to get a hold of money illegitimately.

Another way is they may, or another reason is they, for instance, might want to make a copy of every piece of email that was going in and out from an email server. And in that case, the email could be delivered ultimately to where it's supposed to go, but this bad guy sits in the middle, and literally makes a copy of everything that is sent in and out of it.

And, you know, there is some sensitive stuff that happens there at this point. But the bottom line to why would anybody want to steal or substitute DNS information, is so they can do bad things, or do things to applications, and the applications won't, in most cases, know any difference at all.

So, what are the ways of doing it? Dan already mentioned a bunch of them. They can placed in… There are different techniques. They can be applied to accomplish this. And in fact, one time when I was searching in sort of a general search across the web, to find what people were saying about DNS and DNS hijacking, I happened to come across a university website that had, as part of a particular course, they were asking their students to write software that would hijack DNS.

That was literally a part of the course requirement. So, no mention of any ethics in that either. But anyway I found that rather interesting, but there is a lot of people that know how to do it. There is also a lot of open source software out there that's available for doing it.

So, what is it that DNSSEC is actually doing? You saw in the skit how the star that we used as representation, there is cryptographic mechanisms that are incorporated into DNS and the DNS content that allows the DNS servers and DNS resolvers to determine from a cryptographic basis, if the bits that they get at the resolver are the correct bits that were put in and signed by the originator.

That's really the bottom line. The things weren't mucked with, or substituted as the answer for the DNS question, got asked and responded across the network. So on the next set of slides, this actually shows the sequence of events that more or less mirrors what we did in the skit. The first one is the recursive ISP request.

The next one is stepping through the requests to the other various DNS servers. And then eventually the user gets an answer back. And as hoped, the user goes to the right place. So what happens when that doesn't go so well? Oops.

I have my sequence slightly wrong here. When you get your answer, you get to the right web page. If you're doing DNSSEC and it's enabled, you can some indications sometimes, sometimes not, depending on how your browser is configured. And in other cases, you know, the content is the same as some of the indicators may be different.

And so if Dr. Evil shows up, and in this case, the hijack location is done locally. In other words, the picture is just easier to draw that way, and it can happen in a bunch of different places. But this would be like when you're sitting in an open wireless environment, and somebody else is in that wireless environment, and is monitoring your DNS queries.

Dr. Evil can do that. So, the user, Joe User sends his request. Dr. Evil sees his request, and in this case, he's going to provide the answer before the request even gets to the real servers. And so, Dr. Evil answers, and as we talked about in the skit, the resolver takes the first answer he gets, hands it back to the user, and the user goes, oops, wrong place, but that is where the user goes, because that's what his resolver told his applications.

In the meantime, the actual answer is floating around in the ether, but it will come back, but it will be ignored. So, the bad guy has inserted himself into what the Joe User is trying to accomplish. So we'll… When you get… When you have an arrangement where you can get on your browser some indication, and this just shows one.

There are other ways that you can get it. But this indication is up here at the top to say, okay, you're doing DNSSEC, and you've got to the proper place. There are some plug-ins for FireFox in particular, and I think Chrome also, that will put an indicator up here in the URL bar.

But people often don't use those, but they are available. If you don't use it, you get an indication that says, oh, golly, you're not getting DNSSEC back, and in this case, you can see that the top story was Comcast, the DNSSEC story.

This is actually a screenshot from a real-life hijack that we get for a workshop we were involved with. And the substituted information was actually added to the web page. We didn't replace anything on the webpage, we added stuff to the webpage. And the story that we added was a fictitious one where Steve Crocker admits that the DNSSEC won't solve world hunger.

And one of the things I like to point out is that when a user does one query, they often produce the DNSSEC servers, placing many, many queries across the Internet. Anyone of these, or multiple of them, can be hijacked. Now that last one was CNN dot com, about five or six years ago, and this is CNN dot com about two years ago.

So you can see, there are even more queries than in the past, and you can have a hijack of any one of those, or a substitution for any one of those. So the thing that is, that I want to make it a foot stop, or [inaudible], what is DNSSEC do besides the technical description I gave earlier?

DNSSEC protects the zone data. And the most important thing is the zone data itself, because that's really where your content, that's where your answer is, that's what tells you applications, go to the right place. So here is a picture, another illustration, of places where parts of DNSSEC come into play.

And when you put your DNSSEC into play, depending on each person in this room, you may deal with DNS somewhat differently, and you may have DNSSEC aspects that need to be done different then the person sitting next to you. So if you're just an application user, you need to do what you can to make sure you have applications as best you can, that will make use of it, or that your service provider.

And if we're at an ICANN meeting, and we're using the ICANN provided recursive resolvers, I'm pretty sure we are getting DNSSEC validation here, at the ICANN meeting. There are some other major ISPs that are doing that, so this is all very good. You want see any indication on your application, but you're getting DNSSEC service.

But when you're at home, your ISP may not be doing that. If you're at the office, your business recursive resolver may not doing that. So these are the questions that you, as the user, want to start asking. Am I getting DNSSEC resolution on my DNS queries?

So, you know you're going to the right place. So, there is, like I said earlier, I'm not going to go into all of the word, but there are a large number of places in which different steps need to be taken. If you're a large enterprise that, for instance, is in the DNS business, oh we'll just pick on somebody like ICANN.

ICANN has taken DNSSEC very serious, and has incorporated it into pretty much all of the aspects that they're doing. I happen to work for a fairly large company, whose primary business is not really security technology, it really is a range of technical things, but not IT.

They have done part of the steps. Their external website is signed. Their external names are all signed. This is great. Great beginning. But it doesn't give me resolution right to my desk, so I run my own DNSSEC validation on my own machine. So this may also be something some others may encounter. If you're in, say, a coffee shop, using the open Wi-Fi, chances are almost zero that you will be getting DNSSEC validation.

And this is the kind of place where you are very susceptible to attacks. So one must be very careful there. Now, if you're a big operation that runs around DNS, you're probably going to have people in place… Yeah. People in place to take care of the DNS things.

If you're not, if you're a user, you want to ask for it from the people that are providing your service. But again, the most important thing is protecting the data. That's why DNSSEC was invented, to protect the data. Protect the zone data if you're an operator, whether you're an ISP, or registrar, registry, make sure you are taking proper steps for the zone content information itself, to be properly protected and signed with DNSSEC.

Because it is the real jewels that are being protected by DNSSEC. It's not the DNSSEC keys, it really is the DNS content data. So when you want to incorporate it, you can have it fairly simple, signing the data that gets put into the authoritative name server, that was what we represented when we did the, within third, as we did the checking.

And then when you do your validation, the information is already there. So, for large organizations that have a varied DNSSEC, or DNS centric centricity to their business, which ICANN meetings tends to draw a lot of those, okay? It is very likely that you may have the expertise in house to do the things you need to do to get DNSSEC in play, in your environment.

If you're not that type of business or activity, if you mostly are a user of services that involve doing DNS things, chances are, you'll have to be going elsewhere for the DNSSEC capability, both in terms of service and software to provide it. But you need to ask, because this has been a problem that getting DNSSEC deployed has faced for many years.

People don't ask for it. And this is one of the things we try to make a strong point at, at the workshops, whether it's the software that you're using in the company, the software that your ISP at home is using. Users need to request DNSSEC from their providers of information.

And that was the very, very quick run through of some of the DNSSEC technical pieces. Dan is coming back up, but we can start with… We want to really encourage questions. Let people ask what they want to know about here.

UNKNOWN SPEAKER: Sorry. What's the acronym exactly mean, DNS? Domain…

DAN YORK: So DNS is the Domain Name System. And then the SSEC part just comes from the security extensions. So SSEC is security. Yeah. DNS security. Do we have a second handheld? There was one floating around here before. If we bring that up too.

Great.

UNKNOWN SPEAKER: I am [inaudible] from Gambia. I would like to ask, is it mentioned that some university students had been given assignments of some sort, on creating tools that can hijack DNS. These are many other issues, like organizing programs and hack-a-thons, and other stuff, where people allowed to create tools that can easily be used to hack systems.

And there any policies or plans in place to address this kind of situations?

RUSS MUNDY: So I guess we can both do it. I mean, the challenge is that right the tools that are used to test, can also be used to attack. And it's really a matter of, you know, we develop all sorts of tools that can be used for very good reasons, to go and test the security systems, to test how strong systems are and all of those.

Those same tools can be used, can be turned around to use on an attack. And that's true across all of the IT industry, right? If any, whether it's, you know, email, whether it's web, whether it's any kind of thing like that, we wind up with situations where tools can be used in either way.

So it really comes back to, comes back at some level to, you know, how can you prosecute somebody? What can you do to catch somebody who is doing those kinds of things? In the case of this particular case, it may be that they're not doing that anymore, because somebody might have said, hello university, that's not exactly the thing we want to be going and doing.

I don't know if you've got…

UNKNOWN SPEAKER: Well, one of the things that I did want to just add to what happened in the talk was that, I have subsequently looked for that same course work and that same sort of information. And it is no longer available out there on the net. So that's good. But when universities in general are looking at building technological expertise in folks, one of the things, and there are professional organizations that also raise this issue, and that is the aspect of it that's sometimes referred to as ethics.

That as Dan said, tools that are developed for testing and determining if things are working properly, can many times be used to do the wrong unintended things. And as people, especially people of a technical bent, are taught how to build tools of that nature, they really ought to have inclusion in that, of ethics to illustrate what you should not do with these kinds of things.

Because many people, honestly, have just never really been exposed to that. Oh gee, this is fun. Let's go see what I can do with it. Where, you know, if part of all of the course work was an ethical aspect, that would be helpful, but it certainly not any guarantees.

UNKNOWN SPEAKER: How about policies on making these tools publically accessible by anybody? Because most of these tools you can easily find them anywhere on the Internet, download them. Even non-technical people can easily just download these tools and play around, hack systems.

Right. But the challenge is how do you, you know, to keep that information open and accessible so that people can use that for testing legitimately their systems. You know, like I use a lot of various tools to test the security of my own system, the security of my network systems, all of those types of things. And the reality is that, you know, people have tried at different times to block access to certain kinds of tools, but they could just put them somewhere else.

You know, it's not anything that you can very easily go and do. It's more, you know, looking at ways to educate people on the right ways to do that, the correct panel [inaudible]. Anybody else want to comment on that from the panelists that are here? Russ and I are standing up front, but we do have this whole other group of people around who have some expertise in that.

Anyone else want to comment on that particular one? No. Okay. I saw a question over here.

MARK: Good evening. My name is Mark [inaudible], I'm with the NextGen program. I would like to know how does the HTTPS protocol interact with DNSSEC? And which part of the chain does it fit? And the whole thing works out?

DAN YORK: Excellent question. So HTTPS is the securing of the communication for HTTP, for the web, for the web protocol. What we often call as TLS, or we used to call SSL. The way that it has worked there. So let's talk about that in a couple of different ways. So first of all, all DNSSEC does, is it ensures the, what we call the integrity of the answers.

Making sure that you're getting the answers out of the DNS that somebody in there. So that's all DNSSEC does. You're getting the correct answer back to say, this is the IP address that you want to use to go there. It does nothing with the confidentiality of your communication.

It just says, this is the right place to go, here is the right answer, you can be sure you're talking to the right place. So it's at that first layer before you go and connect, you're being sure you're connecting to the right place. That's what DNSSEC does. Is it makes sure you are connecting to the right place.

Now, when you go to connect to that right place, that server, and you want to have a secure communication, that's where HTTPS, TLS, SSL, all that, that's where that comes in. Is that you're setting up an encrypted connection to that server to, for instance, do your banking.

So it winds… So that what HTTPS is. So DNSSEC helps make sure you're getting to the right place. HTTPS makes sure that nobody can intercept what you're doing when you're communicating there. Now there is one more place that this comes into, which is, to do that HTTPS, you need to use a TLS certificate. And the question is, how do you know you're getting the correct certificate to set up this encrypted communication?

Right now we have this system of certificate authorities, CAs as their called, that go and sign different certificates, so that you know, in your browser has a list of certificate authorities inside of it. Now that works for the most part, but there are times when any CA can sign a domain for any domain.

So there have been bogus certificates. There have been some cases of that. Something that a number of us are working on here, is something called DANE, which helps you put the DANE protocol lets you put a fingerprint, or an entire certificate, into DNS and sign it with DNSSEC, so that now DNSSEC can help you be sure that you're using the correct certificate.

So, that's a high level view of that. But basically again, DNSSEC makes sure you're talking to the right person, the right server we should say. HTTPS does an encryption to make sure it's confidential, and then this thing called DANE can ensure that you're using the right certificate in part of that. Now, HTTP is also just one of the protocols we talk about on the Internet, right? For the web.

There is a lot of other ones. SMTTP for email, XMPP for Jabber, lots of other different protocols that are used. So DNSSEC makes sure that you're talking to the right place, regardless of what protocol you're using. And then, this thing called DANE can help make sure you're using the right certificate when you get there. Does that help?

Okay.

JULIE HEDLUND: This is Julie Hedlund. And we have a question in the chat room. This question is from Abdul [inaudible], and this person asks, who is from NTRA of Egypt. "Is DNSSEC what we need to secure DNS only? If not, what is needed to secure DNS?"

DAN YORK: I guess it depends upon how you consider, what do you… I guess we can say, the answer is, how do you consider DNS secured? There is a couple of different pieces. The DNSSEC ensures you're getting the correct answer, a correct IP address out of DNS, the correct IP addresses. There are other ways to secure DNSSEC, or DNS.

There is some work happening in the Internet Engineering Taskforce, the IETF, in a working group called deprive, that's looking at securing the connection between your computer and the resolver, because if we go back to our skit, if you remember that Norm was as Joe User, was talking to the ISP. To Wes. Who was sitting over there. There is another attack that an attacker could have come in there in between and tried to get in the way of the resolver, and give another answer back to Norm.

There is another attack there that could exist out there, in some way. And so, this other, there is another effort going underway to encrypt the connection between Joe User and the resolver, so that this last little bit of a connection can be ensured to be secure.

So a couple of different pieces of work. So DNSSEC provides the mechanism to be sure you're getting the information out of DNS, that was put in there, and then other work is going on to do other parts of things on that.

RUSSY MUNDY: And one of the things, Dan, I think would be useful to point out here, is that although these are very important things that need to be done, none of these technical and protocol based solutions, are a replacement for the traditional security for the computer system. Security for the operating system. And so, those aspects often get sort of looked past by those of us that are focused on some of the protocol based security mechanisms.

And in response to the question, it's not exactly clear that the person may mean by security, but one of the important aspects of it is to not forget about what I'll call the traditional things that you do to secure any computer system that would be connected to the Internet. So there is a broad spectrum of things, and the protocol solutions do not replace the traditional secure your computer operating system.

DAN YORK: To your point, there has been a number of these data breaches. There has been a number of hijacked websites and things, and often times, we've looked into those and we found that it's not an issue that would have been solved with DNSSEC, because it was some registrar, or some registry, or somebody who wound up leaving their website form unsecured.

So somebody was able to hijack the web form and break into their servers. So to Russ's point, you know, DNSSEC didn't help because they were compromising the servers. So DNSSEC is another layer in the defense that we have for securing systems. Other questions? I saw a couple of others here.

UNKNOWN SPEAKER: [Inaudible] from Internet Society of Palestine. I'm just wondering, because we as a user or an organization, has to us, why not to move toward the default application of DNSSEC?

DAN YORK: We love that. And we're working on that. But one of the things that we get questions from, and if you go up to your friendly registrar here, and if we had [inaudible] here to pick on, we could, but he will tell us that registrars, when we talked about… The registrar's response is, no one is asking for DNSSEC. So we're not going to do it.

Okay. And we've had that from ISPs. Where we've gone out and said, you know, Mr. ISP, do you realize it would be one line in your configuration file to turn your DNSSEC validators, or your DNS resolvers to turn on DNSSEC validation? You know, that's all you have to do. And they're like, well, nobody is asking for DNSSEC, so we're not going to do it, because we've got 57 other things we want to do first.

So part of what we're talking about, you know, asking people, do that part of it is, talk to your ISPs, talk to your registrars, ask them to have, you know, to have DNSSEC. At least file the tickets. Raise the support ticket, and say hey, we'd like to have this.

RUSS MUNDY: Some very major ISPs have actually done that. Okay, Google is probably the best known, worldwide. When you use the standard addressing for your Google resolver, that Google resolver is doing DNSSEC. If you're within the US, a very, very major ISP in the US, known as Comcast, has done that to all of their resolvers.

So it is happening, it is moving in that direction, and those of us that work in this space, you know, want to stand up and cheer, and give credit, to those people that have done it. And your question about why not make it the default? Is one that we would love to see asked to your local providers. Can't you just make it the default for us?

And there are entities out there that will help people, if they're worried about particular aspects of it. So please, do ask and ask when you get back home.

UNKNOWN SPEAKER: I will do that.

DAN YORK: And Wednesday morning…

UNKNOWN SPEAKER: That's on the agenda.

DAN YORK: Yeah. Wednesday morning when we do the DNSSEC workshop, which you are welcome to attend if you like much more, we have about, it's a six hour session that has a whole series of different presentations around different aspects of that. We'll be talking about statistics at the beginning of it. And one of the things that we talk about to this point is, there is resolvers, the validation has to occur, there is also the signing.

And for a long time, some of the resolvers, the ISPs were saying, why should I validate? Because nobody was signing. And the DNS operators would say, well, why should we sign because nobody is validating? Well now we've moved that significantly. Some of the latest statistics out of APNIC showed that about 14, 15% of all DNSSEC queries globally, are being validated right now, and that's significantly higher in some countries and some parts of things.

Russ mentioned the US and some of the activity there in many parts of Europe. They're doing a lot there in Brazil. NIC dot BR has been driving a lot of that over the years, that has been going on in making this happen. So that's happening. And at the same time, there is a significant amount of signing happening. There is a large amount of, in some domains, Norway just recently had enabled signing on their dot NO domain, and just recently passed the 50% mark of 50% of their dot NO domains are now signed with DNSSEC.

So we're finally seeing some strong momentum, in these things, to make that happen. I saw some other questions. Oh, Wes.

WES: Yeah Dan, you actually, this is Wes [inaudible]. You answer a lot, which is, there are two parts. There is the signing and verification side, and the other side about the signing side is that ICANN itself has done a huge amount of work here, so that the entire new gTLD program, all of the new gTLDs have to be signed by the policy of ICANN.

So there is a lot going on and there is a lot of improvement, but we just have a long way to go, but actually in the last couple of years, I think the ramp up has gone significantly hire. So we're getting there to default.

DAN YORK: And to be clear on the new TLDs, when they come out, they have the top level domain has to be signed. And then, so it has to be. The dot, you know, whatever the, dot whatever, not favorites, but we can pick whatever ones that are there.

Any of the new gTLDs, they have to be signed at the top level. So that whatever that is, okay. Now the second level, the ones that we all register, they don't have to be, but they can be. The first step is your top level has to be signed, and then the other ones can be. So all the new gTLDs, the capacity is there that they can be signed, if your DNS operator will do this, will sign it for you, or you'll sign it, that type of thing.

So anything under the new gTLDs has been there, with the country code TLDs, many of them are signed, but there is still a good chunk of them, about 80 or so, that are left that have, that need to still sign. And ICANN is working with ccTLDs to make that happen, and other organizations are as well.

Other questions? I saw some more floating around. Julie.

JULIE HEDLUND: Thank you Dan. This is Julie Hedlund. We have another question from the room, on the chat room. This is also from Abdul [inaudible] at NTRA in Egypt asks, "Could I implement DNS resolver at my local machine to overcome the issue of a securing connection between me and the ISP resolver?"

DAN YORK: Absolutely. In the ideal world, you know, to have this, the validation take place that we had where norm was asking that question of his resolver, that was, that Wes, it was Wes in this case, you know. There is that connection between Norm and the resolver, where an attacker could get in and do something.

Now, Russ mentioned for instance, Google's public DNS that is out there on the Internet that you can use, and does DNSSEC validation. But now that's an even further distance, a network, where an attacker could conceivably get in, and get in and provide an alternative answer.

In the ideal world, the DNS, the validation would happen as close to Joe User as possible. So it could be on the local machine, and a number of us run that on our local machine. There is some implementations out. There is a tool called DNSSEC Trigger, there is a couple of other different pieces that you can install and run on your local system.

So you can have it on your laptop, or your PC, or whatever else to go and do that. There are some applications that will build in DNSSEC validation inside the app. So it's actually running on your laptop or on your mobile phone, or whatever else, it's actually running validation is occurring inside of the application.

So the answer is that validation can occur in different places, and if it's done as close to the user as possible, it provides the highest level of security. Other questions?

Warren is standing back there with a mic. He wants to give it to somebody.

WARREN: I feel like an idiot. Somebody should ask a question so I can give them a mic.

DAN YORK: Come on, make Warren move. People, somebody. All right. Warren is excited now.

UNKNOWN SPEAKER: Thank you. Just one question. When you're sign your… I am a domain name administrator, domain name server administrator. And when you sign your data with your exchange keys with your ISP or registrar. Do you have to do it every time I change my data? Or just once.

DAN YORK: So there is an initial stage, where you sign it. You generate keys, and you sign the records in the zone. And then you start publishing… What happens with DNSSEC, if you're a DNS administrator, then you'll know what happens is there is some additional records called RR Sig, which is resource record signatures.

There is additional DNS records that are created and published on your server. So, your, so you create keys once, you start signing your records.

Now if you change some of those records, you would need to generate a new signature locally on your machine, for those, you know… If you changed your A records, or your quad A records, or something like that, you would generate another signature and start publishing that signature.

But you wouldn't have to update your keys, and you wouldn't have to communicate to the upper servers, you would just do the signatures there and start publishing those, on your DNS server. And if you have slave servers, it gets a little bit more complicated. But that's basically the situation there.

RUSS MUNDY: But you do have to communicate initially with your next higher up, in the DNS chain, to get what's known as DNS record published by your parent. And then if you're using the combination of zone signer keys, and key signer keys, you don't have to ever communicate further with your parent, unless you change your key signing keys.

DAN YORK: You're welcome. Somebody else. Make Warren run.

UNKNOWN SPEAKER: Someone else must have a question. See, that was easy.

JULIE HEDLUND: Thank you. This is Julie Hedlund. We have a question from the chat. This is from [inaudible], and he is from [inaudible], which is an ISP in Argentina. He says, "Is there a best practice guide to implement DNSSEC. If it exists, could you please provide a link to it? Thanks a lot."

DAN YORK: Absolutely. There are a couple in fact. There is a RFC that's called, I do know the number of that folks, quick test. Best operational practices for DNSSEC. 50 something, oh, come on. We've got computers over here. I'm looking at Wes. All right.

So the answer to the question is yes, there are a couple of guides that are out there to help with best practices. There is a RFC that was published that provides a number of different items that are there.

UNKNOWN SPEAKER: 67 81.

DAN YORK: 67 81. RFC 67 81 is a best practices document that is there. Wes actually offered… Actually that was for [inaudible], never mind. Getting ahead of myself. There is also…

I was about to say that. If the person in the chat, Julie, if he or she will go to the slides, or the page for this session, you all should have a document, which is this one here. This, it was on your seats that you have there, or it's floating around, or there is extra copies on the seats.

On the back, there is a whole list of resources that are out there. Some of them are from the Internet Society, the deploy 360 program which has a whole series of different tutorials and other information. There is the DNSSEC tools project, a number of other different pieces that are on here.

So this information is there, and to the person who is listening remotely, you can go to the page for this session, and at the bottom of it, there is the list of handouts, and this is the DNSSEC for the session notes handout, and the second page has all of those links.

And you know what? We should actually add RFC 67 81 to the back of this page, shouldn't we? There we go. All right. Note for next time. Anything else? Back there.

Oh I bet I know what she's going to say.

VICKY: You must have a guilty conscious. Vicky [inaudible] from IFC, we're the bind publishers, we also have a new DNSSEC guide if you're using bind, and you're trying to implement DNSSEC with that. It's published on our website. Possibly with a bribe, I can get Dan to link to it too.

DAN YORK: Yes. So that's the IFC, the folks who are behind bind. And Warren, there is somebody over here too. To get you a workout there. Look at

Warren go. And the IFC folks have done a great job with putting that documentation together, to help people who use bind.

This gentlemen right there, there he is.

UNKNOWN SPEAKER: My name is [inaudible]. Thank you very much for this good session. My question is, do you have any experience about how many person the DNSSEC increases the DNS load? And how long it delays the DNS answering? Thank you.

DAN YORK: Do you want to…? No. So the answer is, that yes, there are statistics out there. I don't have them off the top of my head on that. You're looking at me like…

UNKNOWN SPEAKER: I have some of them, or at least, I vaguely remember some of them. It depends on how you're defining load. The CPU load seems to be, and it all depends upon what software, but nothing more than sort of 2%. The bandwidth load does increase somewhat more than that. But I think it was, it depends on how many zones are signed, how many for using it.

People I think were saying about 5 to 7% on average. I think is what people were saying. But it does again depend on how many of your zones are signed, how many of the people who are querying, you are doing validation, etc. But the load is a lot less than most people would expect.

And the server latency increases, so it's basically immeasurable, so it's a tiny response.

UNKNOWN SPEAKER: There is a memory cost too. But most servers don't need to upgrade in order to do it. So if you're running a DNS server, it's very rare that people actually have to deploy new hardware. If you do, it's because you're running a major one in the first place.

UNKNOWN SPEAKER: Yeah, in the earlier days of DNSSEC there were a good number of reports around this because it was seen as a much larger, seen as a large concern. And so there was a lot of statistics and interest in that. In the intervening years, it's been seen to be not really much of an issue for people to deploy DNSSEC.

And so we haven't really had much done that I'm aware on of stats in the last, like that, on load stats, just because it's generally been seen to be pretty good. Jeff Houston out of APNIC has put together some stats from time to time about the load that can be generated from errors, and some of the pieces that he has done and some of his research about what can happen people do zone signing incorrectly, and some pieces like that, and the blow back that can happen if you've done it wrong, and some of the places that can happen with that.

But otherwise the general load has been pretty solid, from what I've seen. Is there somebody back here? No? Anybody else?

Run Warren run.

Anyone else?

MARK: Hello. My name is Mark. In the name of security, and why does ICE not switch DNSSEC validation on as a default, and actually force people to switch it off if they really choose to?

DAN YORK: Well Warren, you have to bring the mic back to Vicky.

WARREN: I'm giving her some time to prepare.

VICKY: I'm going to take more than that time to prepare. I don't have a good answer for that. Every time we change the default in bind, it impacts a lot of people who are just upgrading to get a particular bug fixed. And are surprised by changes in the default setting.

So we try to be extremely conservative about that. Just take it as a vote for a change in the defaults, but we do change our defaults from time to time, and invariably when we make a change like that, some people are taken by surprise, and it's not…

Yeah, well, as you know, there are two sides to that.

DAN YORK: Thank you Vicky. Not to put you on the spot but, Mark just did. So Julie.

JULIE HEDLUND: This is Julie Hedlund. We have another question from the chat room. This is also is from [inaudible] from NTRA of Egypt. Message size will be increased in case of using DNSSEC, and this may be dropped by firewall. So how can we resolve this issue?

DAN YORK: Yes, so the message size does increase, because when you go and add a signature to it, there are additional records that need to be brought back. And the, what he's talking about with the firewall, can be the [inaudible], right, the records that can be dropped if it goes beyond a certain size.

Yes, that is a challenge that we're seeing out there in some spaces. Again, actually Jeff Houston from APNIC did some research recently around the EDNSO, the penetration of that. And I don't have the stats off hand. You can go and search for them on Jeff on what's there.

But it is one of those issues, but what's happened is that we're seeing an overall DNS infrastructure, that we need to start letting this type of packets through firewalls and such. And so, with this general need, is causing more firewall vendors to make that more accessible. But it is something that is a concern in some places. Russel.

RUSSEL: Yes. This is something that has been a concern for a number of years. And the ICANN security and stability advisory committee, SSAC, probably nearly 10 years ago, certainly seven or eight, issued a report related to this, and I think it has a number of about SAC 35 or SAC 37. Something of that nature.

That there was some testing conducted and there was some identification of some of the procedures and mechanisms that can be applied to a particular situation. And so it's, it is a condition that you do not want to just ignore. You need to think about it, as you're doing DNSSEC related things.

But it's, as with many things, with DNSSEC, this is a set of things that have been looked at, a fair bit has been written about it, and so there is help as to how you should go about attacking and resolving this kind of problem, but the short version is, if you can identify where you're going to be planning to do DNSSEC, do testing before you actually implement it to find out if your firewalls are other middle boxes are going to do bad things to the DNSSEC implementation.

JULIE HEDLUND: I actually have some follow up comments related to this issue in the chat room from someone named Jeff H. Might be… Might be, I'm not sure.

DAN YORK: Hi Jeff.

JULIE HEDLUND: So…

DAN YORK: That would be Jeff Houston for everybody else, who is at APNIC, we're assuming.

JULIE HEDLUND: So Jeff H. says, "Around 7% of queries will fall back to TCP if the response size gets close to 1500." [Inaudible] says, "Yes, Jeff for IDN domain names, the size will be more than 1500." Jeff H. says, "When the response is over 1500 octets, the amount of TCP file back will increase to 10%. The lost rate for smaller than 1500 is around 0.04%."

And Jeff H. says, "High room."

DAN YORK: And I wonder how our Spanish and Portuguese translators enjoyed that little bit of…

We do have a bank of translators back here for the folks who are remote, and it's great to have them here. Other questions?

Okay. Well then, I think what we will do is we'll just finish up with a couple of last minute little slides. Just to say, you know, as we talk about here, just to leave you with some ideas about how you can do something when you go forward from here. One thing is that if you are an operator of a TLD, and if the… If you operate a top level domain in some form, one of the things you can do is sign your TLD.

A basic idea. And we mentioned, all of the new TLDs have to do this. A good number of the ccTLDs have done this. But more need to. Another step you can take is to accept these, what are called, Russ called them the DS records. The signature from the person who signs. So if this gentlemen over here, if they, if you sign your domain, then the next step is to go and have somebody be able to accept that record.

Working with the registrars, helping with statistics. These slides are also available from the web page for this too as well. If you're a DNS operator, well actually, if you have a zone in some form, sign your zone. Check with your registrar that they support DNSSEC. If they do, you might be able to enter the key in there, the DS record.

And ask them for it. Again, we're asking for people to help with statistics, to help let us know what's there. Network service providers, ISPs, the basic step that you can do is deploy a DNSSEC validator resolver, which honestly, might be as little as changing a line in a configuration file.

Vicky, it's what? One line, right?

It's a line or so for bind, okay. For other ones that are outside, for unbound, for power DNS, for some of the different tools that are out there to do that, it's maybe a line or two type of thing. Microsoft server, Windows server. If I have that right. Whatever the name is, they all provide different kinds level that. We also encourage people to talk about this protocol we call DANE. And we have some more information around that, which helps provide an extra layer to TLS certificates, when we get into HTTPS and other things like that.

If you're website content provider again, signing your zones, helping promote DANE in some way, looking at getting those DNSSEC resolvers out there. And again, we'd like to say, using DNSSEC in some way, helping share. You're also welcome, if you're interested, to come to our longer workshop on Wednesday.

The agenda is up on the site, which you can see. We have a series of different topics and conversations. The morning starts with talking about what's happening with DNSSEC in Latin America, with a number of presentations about what's going in this region. We go through a number of different tools. We go and we have a lunch. We talk about some demonstrations that people will show about some ways that DNSSEC and DANE are being used to increase the overall security of the Internet.

So, a lot of different topics on that regard. We'd also encourage you, if you are doing something with it, to, and if you come to ICANN meetings, consider presenting at our DNSSEC workshop. We're always looking for new cases of lessons learned, of new ideas, of new things people have done.

So we'd love to hear from you. When this event is over, we'll be putting out a call for participation for the Dublin event. We'll be putting it out in the next few weeks. And we would, again, welcome people to participate in the DNSSEC workshop on Wednesday of the Dublin meeting at ICANN 54.

So with that, I want to say thank you to all of the folks who were part of this. And you can get more information at DNSSEC deployment dot ORG, [inaudible] dot ORG slash deploy 360. There is a dot ORG in there.

And DNSSEC dash tools dot ORG are all sites that you can have. Yeah, there is no dot Internet society new gTLD.

And with that, I'll say thank you very much. Please do take those sheets of paper that have the information on the back. And we are around, oh… Julie has got one more.

JULIE HEDLUND: This is Julie Hedlund. We do have one more question from the room from [inaudible]. Asking, "Could we have more information about DANE and TLSA?"

DAN YORK: Sure. The answer is we'd be glad to do that if he wants to give an email address, he or she, we can certainly get back to him or her with that information. You can also just go to the deploy 360 website. There is a link there for DANE, and you can get more information about that. Or actually, the DNSSEC deployment dot ORG site has a link there for DANE as well.

And Wes, it's looking like you want to say something.

WES: Yes. So Wes again. Also we will be discussing it on Wednesday so if you tune into that session, the all day session on Wednesday, it will be discussed there. As well as if you go through YouTube, you will find the talk I gave at LACNIC on specifically about DANE. So it's a good half an hour long, about all about what DANE is and how it's used.

DAN YORK: Yup. And if you look at the agenda, it will be in the afternoon of the DNSSEC workshop. We have a whole series of tutorials or demos around DANE and what's involved with that.

All right. Any last chance for questions before we end.

Oh, yes, go ahead.

UNKNOWN SPEAKER: My last question is, who among you is Norm Ritchie?

DAN YORK: Norm Ritchie is right there. That's an easy question. We can answer that one. And on that note, we want to say thank you very much.

Please, we've got folks around. You're welcome to come and ask us more questions. And thank you for being here.

[END OF TRANSCRIPTION]