LOS ANGELES – DNSSEC for Everybody: A Beginner's Guide
Monday, October 13, 2014 – 17:00 to 18:30
ICANN – Los Angeles, USA

UNIDENTIFIED FEMALE: This is the timestamp for DNSSEC for Everybody: A Beginner's Guide. In Pacific, it is 16:55 on October 13, 2014.

JULIE HEDLUND: Good afternoon, everyone. We will be starting the DNSSEC for Everybody: A Beginner's Guide, in about five minutes. In the meantime, we do still have more seats here at the table, and we encourage people to sit at the table. It's much nicer for interaction. So please do come to the table. And also, because we expect more people will join us, so we do want to have as many seats available as possible. So in about five minutes, we'll start. And thank you very much.

DAN YORK: Good afternoon. How's everyone doing today? Good? Enjoying your first day here at ICANN? All right, we've got to have a little bit more interaction than this, right? Hello? Excited? All right. There are a few more seats up at the table, if you'd like to come join us up here.

Welcome to the DNSSEC for Everybody: A Beginner's Guide. Let me ask you first, how many of you know anything about DNSSEC? A few people, all right, good. How many people have signed a domain with DNSSEC. All right, you guys don't count. Okay. How many of you do DNSSEC validation? All right, a couple people, all right. Why are you here?

UNIDENTIFIED MALE: I can leave.

DAN YORK: All right. So in this next hour and a half, we've got a fun program that we're going to talk to you about. My name is Dan York. I'm with The Internet Society, and I'm also part of the program committee that puts on the DNSSEC workshop on Wednesday.

Now, on Wednesday we have a long session that starts at 8:30 in the morning and goes until 2:45 in the afternoon, with a whole series of deep technical dives around DNSSEC. And if you're interested, coming out of this, in knowing a bit more, you can look at the agenda and you can see all the different presentations that we have coming up at that event. We have some about DNSSEC in various different operating systems. We have DNSSEC in North America. We have some pieces about DNSSEC in DANE, in e-mail. So it's a very good series of sessions that we're going to do.

Today, we have a smaller agenda. We have a more concise piece of things here, and we also do have a skit. If you've been promised the entertainment value, we will say it is here. These fine gentlemen who are over here are going to be providing that for you. I'm out of it this time, which is – all right.

You should get one of these, the session handouts. They were floating around. You should see some. We do have a few more if you need any. But you should see those. This gives, basically, some of the speakers who are here and shows you a schedule of what we're going to be doing. And on the back, there's also a whole series of resources that are there. If you don't have a copy, you can go up onto the ICANN website for this session, to the session for this agenda and you will see that you can download the handout there, and you can be able to see this as well.

We do have people attending remotely. We planned this session to have a big period of questions, a Q & A session. That's always been one of the most popular times that we've had this. So we will be repeating the questions back. If you're asking them out them out there, we're bringing the microphone to you so that you can ask the question so that the remote attendees can hear it.

This is also being recorded as well. And so if you find value in this and would like other people to see it, they can go and watch the recording of this once it's done.

So I think those are most of the procedural things I have to say, right, Julie? This is Julie Hedlund, who is the amazing person who has helped us put this whole thing together and keeps us on track and going with this.

So here's a bit of the schedule, as I said. We're going to first have a little bit of instruction, go for some of the DNS Basics part. We have this little skit we'll be doing. Russ Mundy is then going to come up and talk a little bit more in detail about some of the attacks that DNSSEC prevents and some of the ways that it works. And then we like to have this part at the end. It says two minutes, but in reality this is the longer part, where we have a lot questions that we typically like to ask and do that.

Okay. So we want to take a little step back and talk about what you could see as potentially the origins of DNSSEC, as we have it saying here, at 5000 B.C.

This is Ugwina. As you can see, it says, "She lives in a cave on the edge of the Grand Canyon." And this is Og. He lives on the other side. It's a long way down and around, and they don't get to see each other much. They do now and then. They make that trip. And they see the smoke coming from the fire one time, and they said, "Hey, we could send each other messages with the smoke."

So they're starting to use these smoke signals to chat back and forth to each other, from one side of the canyon to the other. And then something bad happens. The mischievous caveman Kaminsky moves in next door, and he starts sending his smoke signals too. So now poor Ugwina, on the other side of the canyon, is sitting there trying to figure out, "Whose conversation do I believe? Who's got the real answers for me at this point?"

So she decides to go over to the other side and try to figure out which of these two signals is the one that she should be trusting. How could she know? Well, while the go over there, she and Og consult the village elders. And as you can see, caveman Diffie thinks he might have an idea. So he goes into the back of the cave. He goes back into Og's cave. They don't know what he's doing. But he comes out in a minute with some strangely colored sand. It only exists in Og's cave and nowhere else, just in there. He comes out there and he throws it on the fire, and the smoke turns into blue. We've got this blue smoke coming out there.

So all of a sudden, now Ugwina and Og can chat perfectly fine, because she can know that the blue smoke is the one that she has to pay attention to, and nobody else. Kaminsky can sit there and try to interfere, but he doesn't have that magic sand that only Og has. And so he can't interfere with this kind of communication. She knows what's there.

That, in a nutshell, is what we're trying to do with DNSSEC. We're trying to give you the blue smoke that says that this is the correct answers, so that when you are looking for answers out of DNS, you know that those are the correct answers. That's what DNSSEC is all about, in a little bit. It's making sure that the information you get out of DNS is information that somebody put in there.

So next up, I think I pass it to Mr. Arends to give a little bit more of an introduction.

ROY ARENDS: Thank you, Dan. My name is Roy Arends. I work for Nominet. I'm going to continue with this presentation. It says, "Introduction to DNSSEC," but let's start with an introduction into DNS. Higher? Is this better? Higher is better. Okay, note to self.

So when you look at the domain name, like www.Example.com, what it actually is, it's a path. And the path can be read from right to left. So there's an invisible dot on the right side of your domain name, and that invisible dot is what we like to call the root zone. Next up in the path, from right to left is, for instance, com. And the next label, from right to left, is BigBank.

This is how DNS actually works. If you have a resolver, the resolver knows where the root servers are. And if you're behind your laptop, your laptop sends a request to this big ISP's resolver. The ISP's resolver, on behalf of the client, then goes first to the root zone. The root zone basically gives out a delegation for the com zone. And now the resolver then goes to the com zone. It then gets a delegation for, for instance, BigBank.com, and it goes to the servers of BigBank.com.

This is how the entire name space can be fragmented into a very, very scalable solution. We can actually play this out in real life with actors wearing t-shirts. So this is just a note to self, if you're interested in how it all works. Let's do a skit.

So I'm going to be the root. We have a few friends of ours. We have Warren Kumari of Google. He's going to be com. Hmm.

UNIDENTIFIED MALE: Very appropriate.

ROY ARENDS: Wes Hardaker, from Parsons, is going to be the ISP. Russ Mundy, also from Parsons, is going to be BigBank.com. And we have Norm Ritchie, who's going to be Joe User. Joe, take it away.

NORM RITCHIE: Thank you, Roy. Okay. So here we have the DNSSEC traveling theatrical troupe. So what we're going to do is we're going to act out what a DNS transaction looks like. So typically, obviously, this happens at lightning speed; very, very, quickly. We're going to do it in slow motion with people. So I need to start with something here. Thank you very much.

So the scenario for this one is this is going to be at typical DNS transaction. This is just what happens every time that you go browsing on the Internet. So in this scenario though, Joe User, I have to do some banking, bills. Okay, so the first thing I'm going to do is go to my laptop. And I'm going to type in, "www.BigBank.com." I'm going to hand this off to my ISP.

WES HARDAKER: Okay, Joe, I'll look that up for you. I don't know where that is. I'm going to ask the root, because the root knows everything.

ROY ARENDS: www.BigBank.com, I have no idea where that is, but I do know where com is. And com is at 1.1.1.1.

WES HARDAKER: Ah, he didn't know everything. I was wrong. But com does. Com, what's www.BigBank.com? Can you tell me, please?

WARREN KUMARI: Sorry, I don’t actually know. However, I do know that BigBank.com is at 2.2.2.2. You should go and ask him.

WES HARDAKER: All right, I will do that. I only have one label left, so this had better end soon.

Hi, BigBank. Do you know where www.BigBank.com is?

ROSS MUNDY: Well, as a matter of fact, I do know where www.BigBank.com is. It is at 2.2.2.3.

WES HARDAKER: Ah, thank you very much. My user will be very happy, if he’s still there.

Joe, I have an answer for you. I have succeeded. It’s at 2.2.2.3. Have fun.

NORM RITCHIE: Oh, thank you very much, Mr. ISP. Now I can go off and do my banking, pay some bills.

So what you saw there is actually what a DNS transaction looks like, more or less, when you type it into your browser. And that’s a standard DNS transaction.

One of the things that’s probably important to remember, me, as Joe User, I didn’t have to worry about much. All I do is talk to my ISP, recursive name server, and he took care of talking to the authority name service, who each knew something about their own piece of the DNS.

So now, next episode of this play, we're going to do what's called a man in the middle attack. So same scenario. I'm going to go off and do some banking. But this time, we'll see what happens here.

Okay. More banking to be done. Oh, more bills; oh, my God. So I'm going to type into my browser, "www.BigBank.com." Mr. ISP?

WES HARDAKER: All right, I've got it for you. I know where to go. Hey, root, I need to get to www.BigBank.com. Do you know where that is?

ROY ARENDS: I know where com is. Com is at 1.1.1.1.

WES HARDAKER: Ah, sounds familiar. I should remember these things.

ROY ARENDS: It's called caching.

WES HARDAKER: Com, www.BigBank.com, do you know where it is?

WARREN KUMARI: Sorry, no. Try and go and ask BigBank.com, 2.2.2.2.

WES HARDAKER: Okay, I'll do that.

Hello, BigBank. Do you know where www.BigBank.com is?

UNIDENTIFIED MALE: I most certainly do. You can find it at 6.6.6.6.

WES HARDAKER: Awesome. My user will be so happy. Thanks.

Here you go. I've got it from the authoritative source. It's at 6.6.6.6.

NORM RITCHIE: Excellent, thank you very much, Mr. ISP. Now I can go off and pay some more bills. Got me.

Now, so that's actually pretty much what happens with man in the middle attack. So what happened there is that Dr. Evil injected a response into the ISP before BigBank did. And Mr. ISP gladly accepted it and gave that off to me.

So, now along comes DNSSEC to save the world. So third act. So what we're going to do now, the first part of DNSSEC is actually an exchange of keys. It's called a Chain of Trust. So one of the things currently is that these servers, they aren't really talking much to each other. They're just saying, "Go there, get the answer." That's about it. They really don't know each other. So they have to establish a Chain of Trust. So that's what we'll do now.

ROY ARENDS: Let's establish a chain of trust.

WARREN KUMARI: Hello. Hi, I'm dot-com, how are you doing?

ROY ARENDS: Hello, dot-com, I'm doing fine.

WARREN KUMARI: [inaudible] I've got a funny hat [inaudible].

ROY ARENDS: Perfect, thank you. I need to have your DS record. I need to certify your signature. So we do this with a handshake, right, and I now take his DS record. That's going to be something I need to use later.

Hello, who are you?

ROSS MUNDY: Ah, I would be BigBank.com. Very nice to meet you.

ROY ARENDS: Okay, I'll try and remember what you look like. Okay, cool.

ROSS MUNDY: Good. So I will hand to you my records to show that I am me and now you know.

[ROY ARENDS]: I will keep track of these. I will make sure that I always keep this with me.

ROSS MUNDY: And here’s this one I will keep on my side of the exchange so that I can use it later.

WES HARDAKER: Well, hello, root. I’d like to get to know you forever.

UNIDENTIFIED MALE: California.

WES HARDAKER: We don’t do rings here. We do stars. Could I have your star, and I’ll memorize it so that I’ll know that you will never, ever lie to me again as long as our stars match?

ROY ARENDS: There you go.

NORM RITCHIE: Okay, beautiful props. I spent a lot of money on this. So now we'll redo that last transaction, the one involving the man in the middle attack. We now have signed zones.

So here we go. More banking. Can you believe it? I had to make a lot of money, because last time I got ripped off. All my money is gone. Okay. More banking. Type in my browser, "www.BigBank.com." Mr. ISP?

WES HARDAKER: Hello, root. Do you know where www.BigBank.com is?

ROY ARENDS: No, but I do know where dot-com is. Dot-com com is at 1.1.1.1, and you can trust this information because here is a signature.

WES HARDAKER: Ah, thank you very much. I recognize that signature. I've seen it before, so I can trust it.

Com, hi, do you know where www.BigBank.com is?

WARREN KUMARI: Sorry, no. I do know where BigBank.com is, though. Let me sign this response.

WES HARDAKER: Ah, thank you very much. I love trusted anchors and stars.

BigBank, do you know where www.BigBank.com is?

UNIDENTIFIED MALE: Yes, I do, definitely. And you can trust me – really, honestly. Here it is: 6.6.6.6.

WES HARDAKER: Do you have a star?

UNIDENTIFIED MALE: No.

WES HARDAKER: Oh, then forget it.

Do you have an answer, other random BigBank.com?

ROSS MUNDY: As matter of fact, I have an answer, and I have a star. This is California, with stars, you know.

WES HARDAKER: And we're on the [Walk of the Stars] street, I believe.

All right, so I have verified that all the stars align and they all match. And because I've verified it against my own star, I know that this is a trustable answer guaranteed not modified by evil people in black cloaks.

NORM RITCHIE: Ah, thank you Mr. ISP. That's stellar. So now I can go off and do my banking, not have to worry about Dr. Evil doing a man in the middle attack on my bank and stealing all my money. So that is our skit. Thank you.

ROY ARENDS: So what just happened? This is La La Land, isn't it? So in short, in reality, what happens, let's say that first skit, where we just exchanged all this information, this happens when you type, for instance, a domain name in your browser, after you press the Enter key and before you see anything on your page. This is how fast DNS, in reality, is.

I think we already did this. Did we go back to the very first slide? Oh, yeah. So I'm just going to skip the Ugwina part again.

High-level concept of DNS, it was invented 1985, almost 30 years ago, I think. There is absolutely no security. Names can be easily spoofed, and caches are easily poisoned. What you've just seen, this is actually fairly trivial to do in DNS.

Actually, we put the skit, all three parts, behind each other. This is what I would normally show in between, so I'm going to skip over that.

So the solution to this problem of cache poisoning is DNSSEC. Now, DNSSEC uses digital signatures to make things safer. So remember that you can put, for instance, an address in the DNS, or you can put an MX record in a DNS. An MX record is what you use when you send mail. You look up the mail host, the mail exchange server.

Now, next to putting an address in the DNS, you can also put a signature in the DNS. It's just another record. Now, these signatures are generated with keys. Keys are just another blop of binary information, which you can again put in the DNS and look it up. Literally, if you want to look up a DNS key instead of an address, you type in, for instance, "Example.com DNS key" if you want to look up the DNS key. Now, since DNS is a lookup system, you can all retrieve this information trivially.

Now, let me just quickly explain in layman's terms. I could explain it to you in proper terms, but I don't want to bore you to death. So the way digital signatures work, public-key cryptography in short, I have a public key that everyone can see. That's the one I'm publishing in DNS. And a private, kind of equivalent key, but not the same. It's a private key. I don't show it to anyone. That's what I'm using to generate signatures. And that's the one I'm not publishing in the DNS.

So remember that a resolver knows where the root servers are. That's actually the only thing a resolver needs to know when it starts doing any DNS lookup. It needs to know where the root servers are. And from then on, it traverses further down the DNS tree, from the root, to com, to BigBank.com.

Now, in that same manner, we can actually delegate trust. The ISP, the resolver, needs to know the public key. It needs to trust the public key of the root zone. The root zone has a hash, basically, a fingerprint of the public key of the com zone, which it then signs.

Com, just like it has an NS record for Example.com, it now also has a DS record, which is nothing other than a fingerprint, of the public key of Example.com. This is the stuff that we did with the stars. The stars are nothing else than this secure delegation part between Example.com and dot-com.

So we did all that. I think I'm done with my set of slides. And this part is going to be done by Russ Mundy of Parsons.

ROSS MUNDY: Thank you, Roy. Okay. And we've succeeded in not having coffee on computers. A little closer. How's that? Okay. Usually I talk loud enough, people like it further away, but okay.

So why are we worried about DNS in the first place? What is it that can go wrong? It's the old, "Ah, nothing can go wrong here." Well, as you saw earlier, how DNS actually bounces a lot of information around between a lot of different pieces, and it all starts in most cases with some end user's computer or some computer that's running some functionality that's sitting out there on the Internet.

And so an end user's computer, whether they're going to their bank like Joe User was, or whether sending e-mail to somebody or Jabber or something else altogether, the first thing that actually occurs is the DNS stuff that we enacted earlier and that Roy was just talking about occurs before you ever see anything on your screen. And so what happens if this doesn’t work right, your applications don’t work right. And essentially everything on the Internet today makes use of DNS.

So why would people ever bother to attack DNS? Well, DNS itself is pretty dull and boring data. It’s just database type of information, with names and numbers and stuff like that. But the important thing is what happens after the information comes out of the DNS and gets back to the one that requested it. Those are the activities that take and make use of that application to go to your bank, to go to your mail server, to go to something else.

You may be riding on a Caltrain train. Believe it or not, some of their control mechanisms run across the Internet. If that’s not enough to scare you off Caltrain trains, I don't know what would be. But there are many things today that over time have migrated onto the Internet and are making use of the Internet technology for speed, for economic purposes. It’s a whale of a lot cheaper in almost every case than building your wires that are connecting all of these things up.

And so that’s why there’s tons of different things out there. And if people decide to hijack your DNS information, they then can hijack your applications that are making use of the DNS information.

One of the interesting things I found a few years ago – and fortunately I have not seen evidence of this going on recently, but this was about five or six years ago – there was actually a university, as part of their classwork assignment, the students had to write DNS hijack software.

That was what they were being taught. And there was no ethics part of it that said, “This is a bad thing to do.” It was, “Hey, you need to learn how to do something like this.” Anyway, there’s at least some set of college students out there that had that as part of their undergraduate degree.

So what does DNSSEC do to help? We showed with the stars and the pictures what goes on is that additional information gets added into the DNS so that the questions that get asked of the DNS come back with answers that can be verified as coming from, first of all, the correct location, like it’s not Dr. Evil; it really is BigBank.com that sent the answer back; and that the information itself hasn’t been changed or messed with or twiddled with in some manner en route.

So from a security geek’s perspective, some people would say it’s [swerves] authenticity and data integrity. So for people that have read a bunch of the security literature, that’s the general security service that DNSSEC actually provides.

The end result is the user knows, or they’ve got techno-confidence that they’re getting the proper answer and their application is going the right place.

So we have just a little example here. And this too is abbreviated, but this is a set of actual packet exchanges that have to occur before the web browser can actually get anywhere. So we’re doing DNS queries to the recursive server. A recursive server goes to, as you saw, several authoritative servers. We’re only showing one here. Comes back, gives the answer back to the user. And then finally the user is able to connect to the World Wide Web server, the web page. And he gets his screen filled. All of this happens, as Roy said, very, very, very quickly. It's not quite the blink of an eye, but it's pretty close. As long as your web browser is doing the things that you are expecting it to do, you would be amazed at how many packets flow behind the scene.

And so what happens if you're doing DNSSEC validation, this is a website that we have that's tailored to facilitate and support DNSSEC. And if you're using a proper browser and you're using DNSSEC, you'll get, in this case, an indication that says, "Yes, indeed, you're using DNSSEC." Or if you go that same website, it'll say, "Oh, no, not using DNSSEC."

So what happens if Dr. Evil shows up? Same set of exchanges. It goes out to the recursive server, but guess what? Before the recursive server can get to the authoritative server, get the answer back to the user, Dr. Evil's already given the answer to the user, and the user's going to the place that Dr. Evil wants him to go to, not the place that the user really wanted to go to.

And so all of this is going on in the background, and even though the packets do come back, they don't do anything, because the software that asked the question, "How do I get to this web server?" has already gotten an answer and it's no longer doing its particular job and it's gone.

So now – oops, am I going backwards? Okay, here we go. Here's an example of an actual website. This is also using one of our websites. And on the left you see the actual content of the website. And this was a couple years ago. Actually, it was about four years ago now. It was right when Comcast made their big announcements about DNSSEC being deployed throughout their network. And that was the stop story that was actually on the website.

But as part of this demonstration, we actually did a hijack. And most people, when you think about doing a hijack, you're thinking about, "Oh, I'm just going to hijack that name up there." Well, yeah, you can do that, and you'll get the whole page. But it'll be pretty obvious probably. If you're doing DNSSEC, the page will be empty and you won't get people going to the wrong place.

But the other thing that you can do is insert fictitious information, which is exactly what we did in this case. We actually hijacked a link that was on the normal website, and looking at it with a browser that did not do DNSSEC, we inserted additional content information. In this case, it was Steve Crocker admitting that DNSSEC would not solve world hunger.

So I've given a single webpage that is going to be doing DNS queries. It does a lot of them. That's from this webpage. And at the time that we did that, there were about, I think, 75 – I counted them once – queries that it actually took to fill a webpage. And all of this happens behind the scenes, when you don't see it.

Now, CNN.com, Weather.com, FoxNews.com, any of the larger commercial-type websites, you're probably talking well over 100 queries, sometimes 200 queries. And any one of those can be hijacked, or multiple ones. That's what the graph looks like today.

So what is it that's important about DNSSEC? Sure, it's the security piece. It's the crypto piece. But what's the most important thing about DNSSEC? It protects DNS data. Okay? Let me say that again. It protects

DNS data so that the users get the information that they need, and they have a way to know that it’s proper. The DNSSEC material is important to accomplish that, but it’s not the reason for doing it.

And so when you do it, it’s different illustration. It shows how a client sends a request off to the recursive server. The recursive server asks the authoritative server. And you’ve seen all this before. And so that’s a very simplified example of how DNS lookups happen. If you think about it, there’s a lot of pieces that make up DNS that you never see. It’s behind the scenes. And so it’s intended to be invisible to the user, which is good. But it is also a lot of places where vulnerabilities can be exploited, which is bad.

So you saw it on our little skit. It can be any one of the queries, any one of the name servers. I showed the illustration of how you can insert content on a webpage. Hundreds, or more, DNS queries to fill a webpage. That can be any one of those, or multiple of them can be hijacked. So it’s a large and complex thing behind it, and so there’s a lot of moving parts. So DNSSEC is the means whereby those parts can be secured.

And so as a user, you have a service provider. You’re making use of some of the big authoritative name servers, root, com, your country code TLD, and a bunch of others. And so you have to be aware of what your part is. If you’re a user, then you should ask for those providers, if they’re doing DNSSEC. And if not, when they’re going to do it. If you’re an operator of one of those facilities, if you’re a manager of a ccTLD – I know we had at least one or two of those in the room here earlier – then they should be the ones that are saying, “We’re going to do

DNSSEC in our ccTLD registry, and we're going to encourage and foster the registrar operators that we work with to also do DNSSEC."

So depending upon where you are in the system, there are a number of places that work needs to be done. And that's one of the reasons we do this, is to help people understand that there are a lot of places and to encourage people to go back and ask for it. Because that's been a challenge for many years, is some of the various providers say, "Nobody is asking for it."

So if you have a large, complex DNS structure and you have your own existing, if you're in the name server business, you have people that know DNS. You can probably do DNSSEC yourself with your resources. And if you want to get some additional ones, they are available. There's a number of people that can help provide the capability to do that.

If you are a large enterprise with many, many locations, you may have a whole mixed environment. You may have products that are sort of commercial, off-the-shelf products that somebody came in and installed for you. You may have some open-source products, and you may have a bunch of other pieces. You need to understand what it is that you're actually doing with your DNS and your DNS business so that you can address all of those pieces.

And so if your activities are just sort of it's important that you have your DNS, but it's not all that critical that it be 100% up 24/7, then it is the same degree of criticality for your DNSSEC protection. So your zone operation, your zone protection, should be consistent with your DNSSEC protection and your DNSSEC operations. And they should all be integrated. And as I said earlier, the important part of all of this is the DNS zone data itself. That's what needs to be preserved, protected.

And so as you think about what you might be doing for DNSSEC, if you're the owner or the operator of some DNS zones, you might also consider what kinds of procedures and processes and care you're giving to the content of your DNS zones and how changes get made to your DNS zones and the actual content itself, because that too is a very critical factor.

So on this picture I drew earlier, the simplest way, in terms of getting some DNSSEC out there, is to have your zone data signed up here and have your recursive resolver – played by [able] person Wes Hardaker, who also happened to be the guy that made this slide. I stole it from you. Anyway, have the recursive resolver or ISP do DNSSEC validation. And as you saw in the skit, then you know from your client that you're getting the proper information back.

So, general principles. If you have a lot in your organization, whatever your organization might be, if you have a lot of important business-critical, business-related DNS activities as part of your business, you probably already have a very strong, very capable DNS set of staff, whether they're organic or contract. However you're doing it, you probably already have people on hand that know a lot about DNS. There's a high likelihood that that set of people can also do DNSSEC, with maybe a little help. But most of the time, they don't need it. There's enough information out there online today they can do it themselves.

If your organization has a very, I'll call it a light involvement with DNS for their critical business functions, you're doing something that, sure, you've got to have a website, you've got to have a mail server. You may have outsourced that. The DNS part is not the core of your business. In that case, the people that you've outsourced it to or the vendor that you're buying the products from are the ones you most likely are going to want to ask to help you do the DNSSEC parts that need to be done. Because they know the products that are being used, the hardware and software, and they're the ones that, if it's going to get done, will probably have the most knowledge of their existing software. So again, like I said earlier, ask for it. Whatever your functions related to DNS are, ask for the DNSSEC capabilities to be added to them.

So that's it for the presentation, and I'll turn it back to Dan for the Q&A.

DAN YORK: Sure. So thank you, Russ, for that. And I'd like to give a round, again, to the folks who did the skit who were here. [applause]

And now we'd like to turn it over to you all to ask some questions. You've seen this. I see some people there. Let me just say too, if there are people remote, you are welcome to join into the Adobe Connect room. Julie is there monitoring the room, and she'll be able to answer that.

And to the panelists who are here, you've got mics here too. So feel free to jump in and answer questions as you wish too.

UNIDENTIFIED MALE: I'll take that one.

DAN YORK: Oh, okay.

UNIDENTIFIED MALE: Or whatever. Whatever [inaudible].

DAN YORK: Somebody. You guys figure it out. All right. So question over there? Yes, feel free.

JOSEPH MARC: Hi, everybody. My name is Joseph Marc. I'm a Fellow from Haiti. Actually, my question is for you guys, [see] DNSSEC for the scalability perspective. As you know, [Internet] things is in its early age. I would like to know if there is already a working group among you guys already thinking about the scalability perspective?

DAN YORK: So the question is with the Internet of Things coming about and all of this, where we're putting IP addresses onto a zillion different devices all over the place and wiring up every light bulb and power socket and machine, or anything else, where does DNSSEC fit into there and what's happening?

JOSEPH MARC: Yes, it's like if I come back with the image that you show, if there is many smoke.

DAN YORK: Right. And it's an interesting question. In fact, the Internet Engineering Task Force, the IETF that works on the standards that underlie all of this, they just established a new – it's a public mailing list for an Internet of Things directorate, they call it. It's a free mailing list you can join for people who are interested in talking about these Internet of Things (IoT) issues when you get into there.

On the DNSSEC side, I don't know that we have a direct answer on that one. Part of the question is what level of identifiers do all of those devices needs? How much are they needing to connect back there, right? That's part of the question.

JOSEPH MARC: Yes, exactly. I am mostly concerned about the payload that will be [had] in the network.

DAN YORK: Right, right. So the level of response that's coming back to all those different devices.

JOSEPH MARC: In terms of latency delays.

DAN YORK: Yep, yep. Go ahead, Russ.

ROSS MUNDY: For, generally, things of this nature that have been assembled out of a lot of individual pieces, one of the things that often happens in that assembly process is places where there's teeny, tiny little things like light bulbs, light switches, whatever that they may not have a DNS name. However, the thing that connects them out to the Internet almost certainly has a DNS name.

And sort of the general principle to keep in mind is anyplace that is making use of DNS should also make use of DNSSEC. I carry around multiple cell phones. And one of the reasons I do that – they run DNSSEC – just to illustrate to people you can run DNSSEC on pretty small devices.

DAN YORK: Yeah, and there are different people who are working on different DNSSEC validation resolvers out there.

Wes, were you going to chime in on this there?

WES HARDAKER: Yeah. so the interesting thing about the Internet of Things is that it's expected to have a gazillion things. And there's really two sides to that, and I think you've touched on one of them. But there's two different realities there.

One, you need to be able to get to random things. So it needs to have a name associated with it, or a statically configured IP address or something, and some way to get to it. So if there's lots of things talking to each other, it's going to get a name. And if they're constantly rebooting and reattaching to networks and changing their address, then they require a lot of dynamic updates. There is a process in DNSSEC for doing that. When you get to the point of millions of them, that may hammer the DNS server a little bit if they're rebooting constantly, but that should be a pretty abnormal case. So I'm not so concerned about that.

On the flip side is them needing to do DNS requests. They're constantly looking for each other. They're constantly looking for other stuff. And that's exactly where a validating, caching resolver comes into play, where they shouldn't be querying the world at large. Because once they know where com is, unlike my example before, where I was constantly going back to com, I would have actually, as an ISP resolver, memorized that, or the local resolver sitting over those Internet of Things. So they won't need to go back and back and back and back. They're just going to go back to the nearest one that needs the answer that they're finally going to get.

DAN YORK: And that's actually an interesting point though we don't do in the skit, but it's one of the greatest threats of the attack, is that if you remember when Dr. Evil gave Wes the wrong answer and Russ gave it back to Norm, the trick in here, what makes it terrible, is that Wes would hold onto that false answer for some period of time, for what's called a time to live (TTL), a certain amount of time in there. And so every time Norm, or this person here, any of the people here, any time they ask Wes for the answer, he'd keep giving them that bogus answer for as long as it was until it expired.

So there's a whole lot of caching that happens inside of DNS, a lot of holding onto those answers and passing them back. We don't show it here in the skit just to make it simple and to do that, but that's part of the reality. But that also helps in that. And it's a good question. I think as we see more happening with DNSSEC and with Internet of Things, I think we'll see much more look at that.

I'll also mention, I see Geoff Huston sitting back there too. And Geoff did a presentation this weekend about DNSSEC measurements and latency and pieces around that. That's available through the DNS-OARC website that's out there, so you can look around for that. Or just say hello to Geoff or look up one of his articles where he talks about this.

Other questions? We've got a mic here too either one of us can run to you. And if you're at the table, you can use these mics too.

CHRIS AUDET: My name is Chris Audet. I'm from the Red River College in Winnipeg, Manitoba. I'm just wondering, what's the best way of advocating to an ISP or your company that implementing DNSSEC is a good idea?

DAN YORK: There's a range of – the first thing to do is to ask them, because one of the questions, like Russ said, we get a lot of pushback from ISPs and people saying, “We don’t get any requests from it.” And so it gets down on their list of stuff to do, and they want to implement this or that. So one of the first things we say is talk to your ISP and say, “When can I get DNSSEC validation? When are you going to turn on” – because the ISPs, what they have to do is they have to be Wes, and they have to start looking for the signatures. They have to start looking for that. That’s what they have to do.

Now, the reality is turning on validation, there’s a great little white paper that SURFnet, from the Netherlands, put out, which shows that it’s just a couple of lines of code for most of the validating resolvers, whether it’s BIND, whether it’s Unbound, whether it’s Microsoft Server, any of those. It’s just this couple lines of code to turn on validation and it starts to go and starts to work that way.

And actually, Geoff’s group is writing some ongoing measurements to show the level of validation. And overall, around the world, we’re seeing about 12% of all DNS queries right now are being validated by DNSSEC. Some are much higher in some countries. Google’s Public DNS has turned it on. So people who use there, 8.8.8 and the IPv6 equivalents, that’s all DNSSEC validated.

Now, what you really want, from a security point of view, you want that validation to happen as close to the end user as possible, because Dr. Evil could still jump in, ideally between Wes and Norm, between the ISP and Joe User. He could still jump in there. So ideally, you want that validation happening as close to you as possible. It could be on the edge of your network. It could be in your operating system.

Do you want to mention Bloodhound, or do you want me to? Russ's team has created a tool called Bloodhound, which is a version of Firefox that does DNSSEC validation, but it does it for all of the different URLs, all the different queries it makes. So it's a fully validating browser [that's] there. There's some plugins that will work with Chrome and Firefox and Opera, and maybe IE I think, that will do validation like on the main website, the main link, but it won't necessarily do it for the 50 zillion other links it has [to pull in]. But anyway, it can happen at different levels.

So the first step is to ask your ISP to get it on there, to do that, and ask your IT department or ask the folks on the edge of your network. There's some guides out there. SURFnet has one. At The Internet Society, we just put up a little two-page document about what DNSSEC is about and how you can get started. There's some resources out there. On the back of this piece of paper, there's some resources there that you can help that have some advocacy resources in there as well.

Russ wants to say something.

WARREN KUMARI: Mic?

ROSS MUNDY: Oh, you're first. Go.

WARREN KUMARI: My mic.

ROSS MUNDY: Go.

WARREN KUMARI: So there are two sort of main parts to it. One is the signing part. And what generally works well is you tell people if they don't sign and they get hijacked, you're going to come along and point and laugh at them. "I told you so. I warned you. You should have done this. You didn't." That way they have some incentive.

The other side is the validation side. And a good tactic there is to say, "If you don't start validating, me and some of your other customers are going to start using other DNS people, like Google's stuff, etc." So a little bit of honey and a little bit of [stick] seems to work well.

And now you can have the mic.

ROSS MUNDY: Thank you, Warren.

WARREN KUMARI: You're welcome.

ROSS MUNDY: Actually, I was going to relate a little bit of my personal approach for doing this. I live in a place in Maryland, on the East Coast, where on the street that I live, I truly have choice between two different vendors. One of them does DNSSEC, one of them does not. I have made it very clear, every time I can come up with a reason to call that other vendor, that the reason that I am not buying Internet service from him, that I'm buying it from his competitor, is because his competitor does Internet standards and, in particular, that it does DNSSEC. Now, I won't name any names, but you can probably guess who those two major vendors might be.

DAN YORK: I see a question right here. But before we get there, I'll just mention two other pieces to that. One is that on Wednesday, if you come to the DNSSEC workshop, you'll hear us talk about something called DANE. And DANE is this really powerful way to add a layer of trust onto TLS/SSL certificates and to provide an additional layer of trust for those certificates, using DNSSEC to do that.

And what we're seeing is we're seeing a lot of interest, especially in e-mail, as a way of providing a higher level of accuracy that you're getting to the correct e-mail servers. And recently, the folks at the CERT/CC in Carnegie Mellon University here in the U.S., they did some research, finding that there are people out there – they haven't yet identified them – who are hijacking e-mail delivery. They're hijacking MX (mail exchange) records, they're routing e-mail through some mail servers, and it appears to be delivered. So it's getting there, they think. But somebody's doing this.

Now, if you had mail servers that are checking for MX records that are DNSSEC signed, the messages would not be hijacked. So there's very real attacks happening out there right now.

CHRIS AUDET: Just to clarify on one last point, if you've deployed DNSSEC on your business network and your ISP hasn't deployed DNSSEC on their DNS server, so you're escalating to the ISP, there's no Chain of Trust to the website. So it wouldn't be deployed correctly? It wouldn't work as expected?

DAN YORK: Well, no. There's two parts to it, again what we said over here. There's the signing side, where you sign your domain. And as part of that, you're going to give, as you saw the guys give their stars, up to the next level. So if you were a dot-edu – or I'm not sure who you are. You would line up to dot-ca or something. Okay. So you would give your signature, or a fingerprint of it, to the dot-ca registry, who would then pass it up. It's all linked that way on the signing side.

On the validation side, every device around here is using somebody for a DNS resolver. They're looking for Wes. If you choose to use the one at the edge of your network, then all of that interaction out there with the top level, all of that, is happening on the edge of your network. And it knows how to get to the root server. So it's all happening there. So it doesn't matter what your ISP does. It's all happening right there.

Did you have a comment here? Over here, she's been waiting for a while.

UNIDENTIFIED MALE: No, no, go ahead.

[ODANA BARIS]: Hi. Good afternoon. My name is [Odana Baris]. I'm from Trinidad and Tobago. I'm a first-time Fellow. I just want to say thank you for that wonderful skit. It was very, very clear – *very, very* clear.

I'm hearing a lot about how spectacular the security that's going to be provided by DNSSEC will be, but I'm not hearing about cost. What is the cost to implement DNSSEC?

WES HARDAKER: Cost is always hard to estimate in some situations like this. The average person will tell you that the cost of the infrastructure is negligible. Anybody that's deployed it knows that it's really not a hit on your CPU. There is a little bump, but nobody's gone out and bought a whole bunch more hardware in order to support this. So that's not really the issue. There is an increase in network bandwidth, but it's nothing compared to your HTTP traffic to YouTube. I'm sorry, it's just nothing.

So there's little, tiny, incremental things. The biggest cost is actually in the education and the understanding. And that's where, in order to understand it – if you turn it on, it's actually fairly easy to turn on, as Dan said earlier. There's only a couple lines of configuration. But it is sort of important to understand how things are going so that you can troubleshoot it when things come around.

So if you actually look at the people that have tried to estimate cost, it's been on the education side, not on the actual deployment side.

ROSS MUNDY: And the Comcast folks have shared with us in various sessions of this nature over time what they did. And although there are a lot of other places around the world that have set up validation for their users, Comcast is country wide in the US. And because they recently merged with NBC, they're now going worldwide. And their intent is to continue to have DNSSEC in place in service for all of their customers, for both the signing side and the validation side. And there was a lot of concern on people's parts within the company, particularly on the validation side, and there have been a couple of instances that have been documented.

But the reality is they thought about this in advance. And as Wes said, the biggest single focus, in terms of what was their cost, was actually training their support staff so they could handle calls that came in with problems. But that's no different than when they stand up any other significant new service. They have to provide the support for it.

WARREN KUMARI: So just really quickly, yes, they did have some support costs, but they've also managed to do a [fair bit] of advertising saying that it's much more secure now. And so the cost of that was offset.

And sorry I cut in front of you, but it was a response. You're going to beat me up after, I [inaudible].

WES HARDAKER: Okay, Dr. Evil, jumping in the middle there. There's another way to look at it, which is how much does your flood insurance cost or your fire insurance cost for your house? And a lot of people end up in the exact same boat in the real-world physical problems, because you don't believe you need flood insurance until your house floods. And then the cost is actually much, much higher than it is to deploy security.

The one that scares me the most – I'll speak more about this on Wednesday. I'm finally glad there's a solution, because the one that has scared me the most for years is that e-mail is the one thing that, once it leaves your ISP, you really don't think about where it goes. And yet there's so many e-mail transactions that nobody actually looks to see if it got to the right server. And you got something and you're reading it, and you certainly don't look in the headers to make sure it didn't go through some person in the middle. And it's one of the easiest ones out there to spoof in DNS and be in the middle, and nobody would notice. Nobody would notice. You get way too much mail to actually look for it.

There's actually finally a solution for that on Wednesday. And for me, the cost of having that be going somewhere else, because it might have credit card numbers in it or whatever that people are putting in mail that they shouldn't, the cost of securing that alone is worth everything else.

DAN YORK: I'll mention too what Wes said at the beginning. And I see a question back there, Julie, we've got there. But before, I'll just say one comment on we said it's easy to get started. Even on the signing side, most of the authoritative name servers, whether it's BIND, whether it's NSD, whether it's Microsoft Windows Server, they've made it now very easy to start signing.

And one of the challenges with DNSSEC is that every time you change your DNS zone, you need to re-sign it, or re-sign at least that part of it. So when you add new servers, when you add new sites, when you change things around, you have to go and re-sign it. But all the software now, the tools have evolved where that just happens. It's called in-line signing. They just do it right away. It all works really nicely. Likewise, the validation is very easy to enable.

But the education point is key, because here's what happened. And Comcast was here four, five – I don't know when, how many sessions ago they talked about this. They turned on validation for their 18 million customers across North America. They did this, and they turned this on. [Everybody is getting this]. The problem came up that somebody at NASA.gov wasn't paying attention to the fact that their key expired. Because one of the challenges, one of the things with DNSSEC, to make it secure, your key expires every so often over a certain period of time. And so somebody at NASA forgot to do a new key. And there's a process around that. I'm simplifying it. But essentially, they forgot that. So all of a sudden, their signature expired.

Well, what happened was people were going on there, they went to NASA.gov, and they couldn't get there because Comcast was saying it's a bad signature, it doesn't work. And they couldn't get a real answer. So they were telling people, "NASA.gov doesn't exist." Well, everybody else was taking out their mobile phones, going on their mobile phones, and they were saying, "Hey, I can get to NASA.gov here. Why can't I get to it on Comcast's network?"

Now, it happened that the day this was going on was that day when there was the whole SOPA/PIPA blackout going on the Net. And so all of a sudden, there was this big, grand conspiracy theory that Comcast was trying to block out NASA, and Twitter was going crazy. And the Comcast guys were going nuts, because they were like, "Wait, wait, wait, stop, we're trying to do a good thing."

So there is that education that you need to do to your customers and to your support people so that they can know what's going on and they can be able to talk to that. And when somebody calls in frantically, "I can't get to that," then they can know to check and see, was this a DNSSEC issue that was going on? There's some education around that.

And there's this operational reality that you have to just have it in your plans that a year from now, or whatever time period you put on there, you need to redo those keys, or whatever period is right there.

I see a gentleman in the back.

[MOHAMED]: Yes, my name is [Mohamed] from [Oracle], and my question is let's say there's a server who uses a SSL certificate to encrypt the communication and it does not use DNSSEC. How can a middle man fake this encryption to the end user?

DAN YORK: To to be clear, DNSSEC doesn't actually do anything with encryption. What it does is it verifies the integrity of the answers that you get back. Now, if you're using TLS/SSL certificate to connect to your bank, if you connect to that server, you're going to get the TLS/SSL certificate and you'll be able to talk to them, you'll have fully encrypted and things like that.

But notice my words: "if you connect to the server." DNS gets involved first. DNS gives you the answers back of where that server is, and you're going to connect to it. So Dr. Evil can jump in there, redirect you to another server that could give you another SSL certificate. So it would look to you – you'd still have that nice happy lock up in your browser, and you'd be thinking, "I'm going to my bank, I'm doing real good," because you've got a fully encrypted SSL/TLS connection. But you've got it to the wrong server.

That's where DNS comes in and DNSSEC. DNSSEC guarantees to you that you're connecting to the right IP address – IPv4 or v6, it doesn't matter, whatever you stick in DNSSEC.

And this thing called DANE that we'll talk about is a way that it can provide an added level of assurance, because you could put a fingerprint of that certificate, or the entire certificate, you could put that in DNS as well. And then your browser could connect to the server, get the SSL certificate from the server. It could also get the SSL certificate from DNS, all signed and secured and stuff to know. It could compare the two of them and say, “Hey, they do match. We’re good. I can fully trust that I’ve got a good connection here.” So that’s what this thing called DANE allows you to do, is to add this extra layer of trust on top of the interaction.

[MOHAMED]: Okay, thank you.

WES HARDAKER: Just really quickly, DNSSEC and TLS or SSL for your web servers are complementary. If you have either one, it’s an improvement. If you have both, you get the double bonus of each step along the way is secured, as opposed to hoping that one is at least the step that’s going to prevent the attacker from doing to you, but you’re really leaving the other one still open.

DAN YORK: I see another question back there. Yes?

[ANNA]: Hi, my name is [Anna]. I was just wondering if there are any studies on the latency implications of implementing DNSSEC.

DAN YORK: You want to hand it to the gentleman in front of you?

GEOFF HUSTON: Geoff Huston, APNIC. Yes, I've just completed some work on this. In terms of using DNSSEC, the most you are going to get, typically, is two extra round-trip times to your local cache. Because in essence, you don't actually do a huge amount more work. You actually need, normally, just two more pieces of information. And beyond that, typically your local resolver has cached all the rest. So it's not a big impost.

And the other thing is if you're actually relying on your local resolver to do all the work, you don't see any additional time in reality. You do a query. You get back an answer with the authority bit set. That's it. It's the resolver that might do an extra bit of work. On average, most of the world does all of its DNSSEC validation within 330-odd milliseconds. Is that fast enough?

DAN YORK: For the remote users, that was Geoff Huston from APNIC, who happens to be sitting in a row in front of the person asking the question.

Other questions? We've got a few more minutes here. Yes?

UNIDENTIFIED MALE: I would like to know how many caves I would communicate safely now. Do you have any road map about the roll-out process of DNSSEC?

DAN YORK: Yes. And, in fact, Wednesday morning we'll have a series of maps out there that show all of the different ccTLDs that are DNSSEC signed. We're up around 540 or so of the 700 and something TLDs are now all signed with DNSSEC. And all the New gTLDs, as part of coming out, they have to be signed with DNSSEC. So we're already going well on that regard.

To not go into too much detail, but there's a couple levels that you get involved with when you get involved [in] a signer. If you register a domain, whoever is hosting that DNS for you, whoever is operating the authoritative name servers, they have to be able to sign the domain. Now, it could be you. You could run your own authoritative name server, and you could do the signing there.

It could be your registrar, who also might do the DNS hosting operator. There's a couple of them out there that they've made DNSSEC so easy that you just go in their services and if you host your domain with them as well, then you just click a little check box. One of the ones I use, I click a check box that says, "Enable DNS," and – boom – I've got DNSSEC for my domain. It works beautifully. They host my DNS as well.

In other cases, it might be a DNS operator, somebody else who's doing it. Dyn, one of the sponsors of the workshop on Wednesday, does a lot of DNS hosting. And they're somebody that will do that, and they'll make DNSSEC very easy.

So step one, as the registrant, as the person doing the domain, whoever operates your domain name for you, whoever hosts those domain records, the zone, they have to do signing.

And then your registrar has to take your records. You [noticed] that we were passing the star up there. They have to take your record, and they have to pass that up to your top-level domain, your TLD. And then your TLD has to have signed, and they have to accept the records. So those are the three pieces: you need the TLD, you need the registrar, and you need the DNS hosting provider.

Now, at the TLD level, we're seeing a good bit of roll-out happening across the world. You'll see some maps on Wednesday morning. Or if you go to the Deploy360 website, which is on the back of there, and you look under DNSSEC, there's a thing that says, "Deployment maps." There are some links there for the latest deployment maps, which show what's happening in the different ccTLDs that are out there.

On the registrar side, the registrars are getting there. With the New gTLD process, an increasing number of them, because they're required under the 2013 Registrar Accreditation Agreement to accept DNSSEC records, they're starting to support more of that. This is again a place, to the gentleman's question here. Go back to your registrar and ask them, "Do you support DNSSEC?" I have one of mine that I keep asking them, and they keep saying, "No, we don't." And I have moved almost all of my domains to another registrar that does support DNSSEC because of that.

And then on the hosting side, you just need to find somebody who can host that. But those are the parts to it. Did that help? Okay.

I think we have time for maybe one or two more questions. I see a gentleman back there. Yep? Right there.

UNIDENTIFIED MALE: So I understand DNSSEC protects from faking name to IP mapping. But I assume the man in the middle can do the same with IP packets, rights? So my question then becomes, it feels that to be secure, I need some kind of certificate on my target, like the bank. And once they have that certificate, it seems I can do without DNSSEC.

DAN YORK: So DNSSEC helps the initial part of that process of ensuring that you are connecting to the correct server. Once you're in a relationship with that server, then, yes, you may want to have an additional layer of security of TLS, SSL, that type of certificate that provides the encryption for your application between your client and the server. So, yes, you may want another layer on there. But DNSSEC helps that first part of getting to the correct server. That's what it does.

WES HARDAKER: Were you asking about the application layer, about how the application secures itself to another application's server, or were you talking about a man in the middle within DNS? I wasn't quite sure from your question.

UNIDENTIFIED MALE: I was trying to understand the difference, like why we care so much about Dr. Evil faking DNS versus Dr. Evil faking IP packets.

WES HARDAKER: All right. That's why I was saying earlier you really need both. You need both forms of security. You need the application-to-application layer security and the DNS-to-DNS layer of security. And Geoff Huston would also tell you that you need the routing-to-routing security, but we're not going to go there today.

DAN YORK: And Julie says she's got a question in the chat room too. Did that help? Did that help? Okay. It's all layers. And DNSSEC is just helping ensure that you get to the correct server. What you do after that and the communication you have with that, yes, an attacker could get into that channel again. It's all layers.

Julie?

JULIE HEDLUND: Thank you. So the question I have in the chat room is from [Pearl2]. And this person asks, "Why do you need DNSSEC at every level? Just to totally secure the traffic? Any other advantages?"

WES HARDAKER: So you need DNSSEC at every level because – well, technically you don't, but it would be a really hard management problem. Because what happens is if – I don't know if there was video of our skit or not.

UNIDENTIFIED MALE: There is.

WES HARDAKER: There was video, okay.

UNIDENTIFIED MALE: There is.

WES HARDAKER: So if there was video, you saw the stars on our shirts. And the one thing – on my shirt, the ISP shirt, there was only one star. And the only certificate that I had to know about and trust was the certificate of the root. And as long as I knew the certificate of the root, I could follow the certificate chain down to anything underneath it and believe anything underneath the root was secure.

If, on the other hand, I didn't want to do it at every level – which is actually how it started a while ago, because the root was signed later than some of the other TLDs – you had to know each TLD, for example. And you had to know all these other certificates, and you had to keep them and maintain them and manage them, and that was a nightmare of a problem.

And what's called the islands of trust problem is where there's other cases where – and I even own a domain, because somebody hasn't update the registrar – where there's a blank spot in the chain and there's no way to get from the root down to this zone that I'm referring to securely, because there's a bump in the middle where there's no pointer, there's no index saying, "This guy is secure. You can use this certificate to talk to him."

So in order to deal with this, I would have to have two stars on my chest, or 15, or 1000, or whatever in order to do that. By doing it from the top down, we only have to have one at the ISP.

DAN YORK: Did they provide a follow-up?

JULIE HEDLUND: No.

DAN YORK: And actually, back to this gentleman's question about the registrar, one of my domains – and that will remain nameless out of not wanting to shame them – they have signed their TLD, but they aren't yet accepting records from registrars. So my domain that ends in dot-something – not that, okay, it's not dot-something, but it ends in that. That is fully signed. It's all signed. And the TLD is signed. But they won't take my records yet. I can't give them my star.

And so when you do that validation, when somebody goes and does that validation, they can't do the whole global Chain of Trust because there's this hole there. They can see it's signed down to the dot-blah, but it's not gone from there down to Dan's domain. So it does require that each of those pieces all agree to accept each other's signatures to make this whole chain work.

WES HARDAKER: Anybody know if dot-something and dot-blah are taken yet?

DAN YORK: I don't know. Next round. We've got time for one or two more actually. I looked at the time. Yes, over there?

VALENTINA PAVEL BURLOIU: Hi, my name is Valentina. I am from Romania, and I'm a second-time ICANN Fellow. I would to turn the discussion to future challenges, because I heard Fadi this morning telling us that although it's unconfirmed yet, China has built its own root zone. And how would DNSSEC not be confused in this scenario?

DAN YORK: Ooh, who wants to touch that one?

VALENTINA PAVEL BURLOIU: Wait, wait, wait. Since I have the microphone, I want to take advantage to put another scenario on the table. In Europe at least, there are some tendencies in favor of creating a parallel Internet, more secure, more private, etc. And this of course means barriers between the networks of networks. And I'm not sure, from a technical and operational point of view, how this can work. But also, how can tools like DNSSEC can still function and provide results?

DAN YORK: Sure, it’s a great question. And we probably have a couple of us who want to weigh in on that, but I see Russ wants to.

ROSS MUNDY: So for many years, a lot of people thought – and it’s really a misimpression – that there can only ever one be one root zone anywhere in existence in the world. Well, that’s just not true. The whole technology that the Internet is built on is used in a bunch of different ways, and there have been a fair number of completely private networks built multiple times in multiple parts of the world. And obviously, the content of the root zone and the TLDs and whatever else is in their DNS is different than the regular Internet root.

So anyone that wants to run an independent network can do so. The problem is most people don’t want their separate network to be separate. They want it to work with all of the rest of the Internet. And they also want to control every piece of content when you have a situation of that nature. And so what you usually have to do is you have to end up deciding which of the two you’re going to do, because you cannot have inner operability and have things work together when the critical identifiers that have to be unique in fact are not unique. And so somebody has to go one way or the other.

And DNSSEC can be used in those private environments as well as the big Internet. But it will tell you, if you’re using a DNSSEC key from one of them and not the other, whether or not the stuff that you get came from the one that you have the key for or not.

DAN YORK: Right. And it goes back to what Wes was saying earlier about when Wes was the ISP and he does validation, he has the key, the trust anchor, that is from the root of DNS. And so he uses that to trace down this global chain of signatures to go and verify that the signature on that zone is correct. So it all rolls back up to there.

So if another organization, another country, another entity were to have a separate Internet, or a separate DNS root I guess you'd say, and you were to go and do DNSSEC validation there, and you only had the trust anchor for the global DNS root, then your DNSSEC validation would fail because it would not work. You could not follow that chain all the way up there. The signatures would work for the individual pieces, but you wouldn't be able to validate that there wasn't something happening in there to go and do that.

And actually, interestingly, we're going to be having a discussion on Wednesday and then again on Thursday about the process that's involved with changing that trust anchor for the root, what's called the Root KSK Rollover. But essentially, how do we change that, if we want to, for the root of DNS? But that means that all those ISPs who are now doing DNSSEC validation have to change that key in some way.

But if you had somebody else doing a completely different root, all of those ISPs would have to get another trust anchor somehow. They'd have to get that onto their systems. They'd have to get signatures that would line up to that other trust anchor. I mean, it could be done, but it would be a very involved process in some way to go and make that all happen. But the DNSSEC technology itself relies on this global Chain of Trust, which right now is based off of the main root key.

I see Wes wanting to weigh in here.

WES HARDAKER: If you look at the problems associated with that, you can actually enumerate them fairly simply. Let's see, I need a fictitious company name, [Blah-eo]. If you're inside [Blah-eo] and the government has blocked DNS so that you can't make queries yourself out of the network, which is likely the case for some real states, the best you can do is – and if they've created their own root, they've created their own DNSSEC key at the top. You'll believe everything in them and you can validate everything in that alternate universe. It's just that you know who can poison your information, because they have they keys to the root and they can fake you all the way down. The best you can do is you can assure that there's nobody else in the country that is messing with you, other than the government.

If you're external to [Blah-eo], who cares? For the rest of us who are outside, it really doesn't affect us at all, because they're inside and they have their own problems, and we're outside and we're not going to see that problem.

The worst case is the people that are transiting, the people that are going in and out. If you're outside and you have the root key from the outside, like Dan was just talking about, nothing inside is going to validate for you if you're taking in a computer that does DNSSEC.

The reverse is also true. If you're on the inside of [Blah-eo] and you only have the key for the inside and you come outside, nothing is going to validate out in the real world. One good advantage is that if you have both keys, you can actually go back and forth. And if you chain to either one, you'll believe it if you want to do that. They're subject to debate as to whether you want to do that when you go inside, but nonetheless.

So the enumeration possibility, it's not an extreme number of cases to actually think about. And there's another interesting one, is that Russia, with the GOST algorithm, is actually doing sort of just that, where it's likely that they're deploying their own trust anchors and their own software for ccTLDs that are underneath. So their software may have a separate trust anchor for the ccTLDs [within sight] of the Russian Empire.

UNIDENTIFIED MALE: Federation.

WES HARDAKER: Federation, thank you. I just got kicked out of the room by like half the audience. And I'm not a politician, and that's why. So there's other cases where people – even in an enterprise, you may want your enterprise dot-com to be a separate key so that you don't have to trust anything up above it. There's nothing wrong with that. It actually still works.

DAN YORK: And on that note, before we have any other political calamities –

WES HARDAKER: Sorry.

DAN YORK: We are drawing to a close here. We would encourage you again, take a look at this sheet that's here. There are some good resources on the back that you can look at. The program that I'm involved with at The Internet Society, called the Deploy360 Program, has a good bit of information there. There's some information for registrars. There's the maps.

There's the DNSSEC-Tools.org site, which has some great resources, some libraries you can use. There's the Bloodhound browser that we talked about, which is something that you can try that does that. There's a number of other things. OpenDNSSEC is a tool that can be used for signing domains and for working on that. There's a great plugin for Firefox and also for Chrome that will show you, it provides another little icon, a little key up in your browser, so you can see whether you go to a site that is actually signing with that. There are some tools from Verisign Labs. There's another bunch of a resource that are out there as well.

With that, we'll draw this to a close and thank you for coming here. The group who are around, we're around here if you'd like to ask us questions. Again, if you're interested in more, we do have a day-long session starting at 8:30 on Wednesday morning, going until 2:45. You can see our agenda up online so you can see the different panels that are part of that.

What?

ROY ARENDS: Just checking, that's a day-long session from 8:30 to 2 –

DAN YORK: All right, okay, it's a six-hour session. Okay, sorry, 6.25.

ROY ARENDS: But you promise it will feel like a full day.

DAN YORK: It will feel like a full – hey, and there's lunch included if you come too. But you can come to the session. You can see on the agenda what's on there. There's some great things about some new tools, about some of the e-mail tools that are there. We've got a good bunch of pieces that are there.

And go out, please, ask people about DNSSEC. See what you can do with it. See if your registrar supports it. See if the DNS hosting operator will provide it, and start asking them why. And let's get it out there to be more deployed, to make a more secure Internet. So thank you for your time.

This will also be recorded. As we said, the recording should be up there at some point soon, so you'll be able to see it, including the skit. Thank you again.

[END OF TRANSCRIPTION]