MONTREAL – DNSSEC for Everybody: A Beginner's Guide
Sunday, November 3, 2019 – 17:00 to 18:30 EDT
ICANN66 | Montréal, Canada

DAN YORK: I would say, we're going to have some questions and answers coming up in a little bit and if you want to come on up, a little bit closer, we're in this massive room here today, so please feel free to come on up. We'll have a microphone; we'll go around and talk to you and do this.

So, my name is Dan York, I'm with the Internet Society involved with some of the technical advocacy work we do there, and what we want to talk about today is, what is DNSSEC, what purpose does it serve? And we're going to do that through a couple ways. We're going to tell you a little story, we're going to act out a skit, a couple of skits, we're going to talk a bit about this, and we're going to try to have a little bit of fun on this Sunday evening.

First of all, may I ask a question? How many of you here have deployed DNSSEC in some way? Okay, a few people, alright. Well, how many people have no idea what DNSSEC is at all? Okay, a couple. I notice the overlap with the folks who deployed that, so there we go, we're good. So we're going to take you back a little bit and tell the story of the origins of DNSSEC in 5,000 BC.

So, as our story goes, this is Ugwina. She lives in a cave on one side of the Grand Canyon and this is Og, he lives in a cave on the other side. It's a long way for them to go back and forth, and so, they don't get to

__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.__

talk too much, or visit, or anything else like this. So, on one of their visits, they notice that there's smoke coming out of Og's fire. And so, they realize that they could chat using smoke signals; they could go and send smoke signals across that they can, obviously, tell each other more stories, talk about this, have much more of a conversation.

But one day a certain another nearby caveman, we'll call him Kaminski, moves in next door to Og and starts to send his own smoke signals. Suddenly, Ugwina on the other side, she can't know which one is the right one; she doesn't know. "Who should I be…? What's the right signals that I should be seeing here?" So, she sets off to try to figure out, "What can we do here? How can we make it work so I can know which one is there?"

So, they go and consult the wise village elders. Caveman Diffie thinks that he might have an idea. He gets up and he runs into Og's cave and he goes to the very back where he sees this pile of blue sand, this strangely colored sand, that only exists in Og's cave. So, he takes some of that, he runs out, and he throws it into the fire. The fire turns into a magnificent blue and suddenly, now Ugwina and Og can chat, because now she knows which one is from Og. Nobody else can interfere, because they know for a fact that the blue smoke is coming from Og, not from somebody else.

In a funny way, this is what DNSSEC is all about. It's about ensuring that you're getting the correct information from the sender. It's doing something special to the information so that you can be able to see what is the unique information coming from that person. So, we're going to talk a bit more, get a bit more technical around this.

At a high level, right, this is how DNS is often portrayed. We wind up with the root of DNS, we have all of these top-level domains, these TLDs that are here, all the different kinds of forms. And then, we have our second-level domains below that. And we have all of this going on. A resolver, a DNS resolver, knows how to get to the root, it knows how to go through the hierarchy, go and figure it, and each level along the way tells the resolver, "Go talk to somebody else."

DNS is a distributed database. It goes and figures out how you get the information from each different resolver, caching it all along the way. But there's no security in the protocol, just as in our little story, somebody else can come along and spoof, can give other answers in a different way. You can poison the caches of those resolvers, because once they store the information, it can be held on for some period of time.

So, we're going to act out now. Is our troupe ready? Come on up. We're going to show you a bit about how this acts out. So, what you're seeing is that you're going to have our characters here that are going to play the role of a user, who is going to want to go and search for information, want to connect to bigbank.com. So, as our troupe is arranging itself. Alright. Wait. Okay. Here we go. Okay. So, Wes Hardaker will be our user, who will talk to our internet service provider, who is a resolver, and that resolver will then interact with our rearranging DNS hierarchy here.

WES HARDAKER: Test, test, test.

FRED BAKER: First problem, we need electricity.

DAN YORK: Audio, can you bring up that mic?

WES HARDAKER: There we go, alright. I think I want to buy a yacht. I've always wanted to buy a yacht. They're great big boats and I like great big boats. I think I'm going to go check my bank and I bank at www.bigbank.com and I'm going to find out how much money I have. Can you please give me the address for www.bigbank.com so I can go talk to it?

WARREN KUMARI: Sure, you're just the sort of customer I like to keep happy. Let me go figure that out for you. Hello root, one of my users would like to go to www.bigbank.com. Can you please tell me where that is?

FRED BAKER: Well, I wish I could, but I've got a problem. I don't actually know. I do know where to find .com, you could ask .com.

WARREN KUMARI: Okay, thanks, I'll give that a try. Hello, .com. One of my users wants to go to www.bigbank.com. Can you please tell me where that is?

UNKNOWN SPEAKER: Well, I'm not sure about www., but I know bigbank.com is just right over there.

WARREN KUMARI: Fine, I'll go ask him. Hello, bigbank. Can you please tell me where www.bigbank.com is?

RUSS MUNDY: Hello, Mr. ISP. I can tell you where www.bigbank.com is, it is at 2.2.2.3.

WARREN KUMARI: Woo, hoo! I finally have an answer. Hello, Mr. User, www.bigbank.com is at 2.2.2.3, and can I come along on your yacht sometime?

WES HARDAKER: I'm afraid my yacht doesn't allow recursive resolvers, but that's okay. Alright, so I can go check -- Wow! I have a boat load of cash.

DAN YORK: Let's give them all a round of applause on that one. So, that's how DNS operates. That's what happens all the time for all of the bazillions of little DNS queries that are going on. But we want to talk a bit more about how this could work. So, we're going to bring up another exchange. We're going to do this again, but this time you're going to see what happens when an attacker gets involved.

WES HARDAKER: Hello, there we go. Today is the day I'm going to buy my boat, my great big yacht. I need to go to bigbank.com again so I can transfer my money, can you tell me where it is again, because I forgot?

WARREN KUMARI: Yeah, sadly I forgot as well. I'll go figure it out for you though. Hello, root. One of my users wants to go to www.bigbank.com. Can you please tell me where that is?

FRED BAKER: If only I knew the answer. I do know where .com is, though. Would that help?

WARREN KUMARI: Eh, yeah. The root's kind of useless, so I'll go ask .com. Hello, .com. One of my users wants to go to www.bigbank.com. Can you please tell me where it is?

UNKNOWN SPEAKER: Well, I still don't know about www., but I know that bigbank.com is at 2.2.2.2.

WARREN KUMARI: I'll go and ask that. Hello…

ANDREW MCCONACHIE: Actually, no, because bigbank.com is at 6.6.6.6.

WARREN KUMARI: Okay, sure. No worries. Hello, Mr. User.

WES HARDAKER: Oh, 6.6.6.6, I know where -- I can go give all of my money to 6.6.6.6, thank you. Where's my boat?

ANDREW MCCONACHIE: Thank you. Ha, ha, ha, ha, ha.

WES HARDAKER: My boat?

DAN YORK: Alright. Let's give them another round. So, this is indeed how DNS, that we all are here to talk about, DNS can be poisoned this way. The attacker can do it. Basically, whoever is able to give the answer back to the resolver first, wins. You know, speed wins in this regard as far as who can go and do theirs.

So, in this case, Dr. Evil was able to get in before poor Russ here was able to go and give an answer back, get that answer there. Now, part of the danger, too, is that now, Warren with the hat, our ISP, he's going to hold on to that answer for some period of time. So, for anybody else who asks where www.bigbank.com is, they're going to continue to get the bad…

ANDREW MCCONACHIE: 6.6.6.6.

DAN YORK: Exactly. They're going to get that bad answer, repeatedly, until it times out. This is DNS attacks. This is cache poisoning. This is all of this, it's there. So, what we now have is, again, this is DNS. With DNSSEC we add in this concept of digital signatures, and you can see our troupe still staying here, because they're going to act this out again in a moment.

What happens is, you have keys and signatures that are stored inside DNS so that you can be able to check, did that information actually come from the original source? Is that really who should be giving out the information for bigbank.com? So, a resolver, to make this all work, a resolver knows where the root key is, or knows how to get that. How many people heard about the root key rollover last year? Yeah, okay. People looking at that.

This was all about ensuring that there's a chain of trust from the root of DNS, all the way down the chain for the different people, different authoritative servers that are providing this information. It all links up so we can protect the integrity of the information that's there. So, we want to make it so that our big bank name server, right here, he can be the one giving out the information to the ISP, not somebody else. So, let's bring up our troupe again, as they are here, and let's have this acted out another time, this time with DNSSEC.

WES HARDAKER: You'll be glad to know this is the last time.

UNKNOWN SPEAKER: First we're going to need signs.

DAN YORK: Oh. Oh, yes. We have to go through this first. Go ahead, guys. So, what are we doing here? The root is signing. Now, wouldn't IANA like it if it was that easy, right? So, you'll notice the root signed theirs, .com is signed, big bank is signed, everybody's all signed. We're good. And now…

WES HARDAKER: Okay, let's pretend that didn't happen. I have another yacht worth of money. I'm going to go buy another boat for realsies this time. Can you tell me where bigbank.com is this time, and can you get it right?

WARREN KUMARI: Yeah, I'll try. Let me go along and ask the root. Hello, root, one of my users wants to figure out where www.bigbank.com is, can you please tell me?

FRED BAKER: No. No, I can’t. But I can tell you where to find .com and .com may be able to tell you that. And I'm signed.

WARREN KUMARI: Let me quickly check that signature. Yeah, okay, that looks valid to me. I'll go along and check with .com. Hello, .com, one of my users still wants to buy a yacht. He needs to know where www.bigbank.com is. Can you please tell me that?

UNKNOWN SPEAKER: I still don't know about www., but I can tell you that bigbank.com is at 2.2.2.2 and I can sign that response.

WARREN KUMARI: Let me check that signature. Yeah, that looks okay, I'll go along and ask that. Hello, www.bigbank.com.

ANDREW MCCONACHIE: Hi.

WARREN KUMARI: Hey, how are you?

ANDREW MCCONACHIE: 6.6.6.6.

WARREN KUMARI: Where's the signature? I don't see the signa [CROSSTALK] Bigbank.com, can you please tell me where www.bigbank.com is?

RUSS MUNDY: Well, I certainly can. www.bigbank.com is at 2.2.2.3 and it is signed.

WARREN KUMARI: Let me check this, and I'm going to check it carefully. Yep, that looks okay. Here you go, user, www.bigbank.com 2.2.2.3 and I validated it, you can trust that.

WES HARDAKER: Oh, thank you. Mr. Bank, can you transfer all of my money to Dan York? I'm buying a used boat from him.

DAN YORK: Why, thank you, Wes. Please give these folks, a round of applause. So, that's how we do it and that's what DNSSEC is all about, is it's having these signatures that ensure that somebody else can't get into that process.

That's what it does. And that's all it does, an important part. It just ensures that the integrity of the information, what was put into DNS is what the user gets out. It's not about confidentiality, it's not about securing that information, it's purely about verifying that the information is exactly what the user put in. Now, to talk a little bit more and go into an example, we're going to bring up Russ Mundy, who is going to come up here, and I'm going to give Wes his money back.

RUSS MUNDY: Thank you, Dan. And thanks, everybody who came to join us this afternoon. Boy, those lights are bright. So, what I want to talk about here, a little bit... Ah, the clicker, good. Is examples and descriptions of the things people need to think about as they go through the process of deploying DNSSEC. Part of the "Why do it?" is, "Why are we worried about DNSSEC to begin with?" And we already talked about it from the DNS perspective and how DNS information gets, can be messed with, particularly if you don't have DNSSEC in place.

But why do people go after DNS? DNS itself is not all that interesting. When people go after doing things to DNS, it's in almost all cases, so that they can do things to applications that are actually doing the DNS queries. So, as you saw earlier, when Wes was wanting to move money around, in that case, it was an effort to steal money. So it really is important for the applications, that make use of DNS, to do what they're doing. So, if it doesn't get to the right place, who knows what's going to happen.

So, we've had multiple examples, in the real world, of things of this nature and just -- Some of the things are identified up there on the board and it's any application that's running on the internet today. There's an extremely high likelihood that it's making use of DNS underneath of it, and most of the time users of applications don't know and frankly don't care that there's DNS present, but it's essential for their applications to function properly.

One of the things that I found a few years ago, and I went back and looked again, and unfortunately, I didn't keep the specifics of what I found. But there was a university professor there that I found in a course on programming that required his students to write a DNS hijack program.

And I looked through the entirety of the course requirements and layouts, and there wasn't a single thing that I could see that talked about ethics or why this was something that you shouldn't do. It was just, “Hey, students. Go write a DNS hijack,” and it was really kind of spooky as somebody that's been trying to keep hijacks from happening for a long time.

Fortunately, I've not been able to find that for about the last five years, so maybe it's gone away. So, as Dan said, that's the important thing is being able to get to the right place, and when you get to the right place, be able to verify that the information you get back is, in fact, correct.

So, the public key cryptography that's embedded to actually make DNSSEC work is the technical mechanism that is underlying of this. Now, when we went through some of our earlier efforts, we did, at ICANN meetings, actually run real hijacks. This is just a series of slides that kind of gives the same idea pictorially with what you saw with the on-stage performance here.

One of the reasons we stopped doing it for real is, at one, in one of the meetings we managed to instead of just hijacking the DNS in the particular room, well, the configuration of the network wasn't quite as expected, and we hijacked the DNS for the entire ICANN meeting. That was quite a laugh when it was over, but it wasn't while it was going on. So, we now just show slides here, and you can see Joe User is down in the lower left-hand corner, and he wants to go to his web server up there.

And you can see, from the picture, he sends off a query. That query, that goes to his recursive server. The recursive server saves, sends it to the authoritative name server associated with the web. His web server he wants to go to gets the answer back to the recursive server. And the recursive server then goes back and tells the user. This was what you saw, us going back and forth, running around on stage doing.

Now we'll put in, after that, then he actually can conduct his transaction. So, when we put in actual websites, this is a particular configuration to a website so that the visual image on the website itself shows if you're doing DNSSEC underneath.

There's no standardized image to show that there's DNSSEC, but it was a whole lot easier to just set it up on a website so you could see it. And when you go to that same website, when you're not using a DNSSEC validation mechanism, you get a different symbol. So, you can see the top one is a checkmark and the bottom one is, you know, a triangular warring to tell you, “Oh, your DNSSEC is off.”

So, when we do the same type of thing, as well, we were showing on the stage here, again, Joe user sends a query, but this time Dr. Evil is on the network. So, the query goes wandering off and, in the real world, what actually happens is Dr. Evil sees the query and provides an answer, even though the query continues to wander through the network, but Joe user is sent off to the impersonating website.

And you can see the other queries went through the network and came back, gave an answer, but Joe user didn't get that answer, because the resolver that he was using took the first answer and went to the wrong website, so he could not get back to there unless he was using DNSSEC. When he was using DNSSEC it prevented the incorrect answer from getting to his resolver, and then afterwards, after he got the correct answer, he went back to the correct website and conducted his business as appropriate.

So, we instrumented a website to show what you can do, and specifically the website was built so that we, there was a section of the website that showed, that was a place where a hijack could occur. And so, the actual hijack that we conducted against a web browser that was not doing DNSSEC, we actually inserted information, and the information we inserted was a bogus story that says, “Steve Crocker admits DNSSEC won't solve world hunger.”

So, it was a fairly obvious and intend to be totally humorous illustration, but if you look at the front most ‘DNSSEC is off’ image and down at the bottom you can see .org shares Comcast DNSSEC advice for ISPs, and on the one at the top of the page, that is the top story. So, essentially, with the hijack we inserted part of information on a page, so even though it was on the same page on the browsers, it was different information and, of course, false information was inserted.

So, on a single web page, how many, you know, from going from an empty name server with no cached information, you know. This is CNN.com from probably six or seven years ago, and there's somewhere around 75 to 100 queries and responses, just to fill one page. So, any one of those could be hijacked, or a large portion of them could be.

Now, has it gotten any better? Not, in some ways yes, in some ways no. There are more queries that it takes to fill a commercial website page than it used to. But this particular instrumentation shows that there are, now, some of those are DNSSEC signed, but the number that it takes to actually fill a website is just about doubled in about four or five years. So, the basic thing that people often get concerned about and think about, when you talk about DNSSEC, is, “Oh my goodness, there's these cryptographic keys. What do we have to do? It's so important for taking care of the crypto keys.”

Well, that's true, but what's most important is your DNS zone data. So, you need to take at least as much care with the accuracy and correctness of your DNS zone data as you do with any crypto keys, because the point of having DNSSEC associated with any zone, is that the user who gets that information knows that the DNS information is correct. And so, if you take more care of your crypto keys than you do of your zone data, and somebody wants to attack your zone, they'll attack the part of your system that does the entering of information into the system.

And if you sign that information, the recipients will say, “Oh, well it must be good, it’s signed,” but if someone successfully attacks, what's often called the 'provisioning side’ of your information, of your DNS part, and gets the inaccurate information in there, in some ways, you're worse off than you were when you weren't using DNSSEC because you, as an operator, are verifying through crypto that that information is correct and if it's not, then it's on you for not handling your information correctly and properly.

So, here's another example of doing DNS without DNSSEC. Zone, for zone data, where you are putting information into your authoritative name server. So, that information goes in, the authoritative name server is there on the internet, running, and contains it, it receives a request from a recursive name server, who has also received a request from a client and it answers that request.

So, if you're including DNS in your operation of your system, as opposed to outsourcing it or having some registry provided for you, if DNS is important enough for your function of what you're operating that you are doing all of the operation within your organic organization itself, you probably have DNS knowledgeable people on staff. And you're probably going to want to do the DNSSEC activities as just part, as extending what you're already doing, to run DNS.

So, large activities operating in their own DNS, especially where DNS is particularly critical, are likely going to want to do their own DNSSEC implementation and operation. So, sort of a big TLD operation that you're registering for, or you're a big enterprise, hp.com has always been a great example here; verisign.com, their business is tied to the DNS, they are important organizations from a DNS perspective, and so, they're going to be doing their own, probably.

If your DNS zones are things that might not be quite so important, either to the internet or to the economic viability of your organization. So, if you're, my example here is that as net-snmp.org, which is domain that I think I own. It's one that doesn't really do anything. Oh, you own it now? Oh, okay. I transferred it to Wes. Okay.

But the fact of the matter is, it's not really a critical DNS operation to -- it's good to be right, but it's not critical to the internet, to your business function. And then, all of us here, we use DNS, we need to make use of DNSSEC when we can. Again, the important thing is to protect the DNS zone data. So, now, we saw the example before, of loading up the authoritative zone and doing the request for information and the answer.

So, this is a nice simple illustration of places that need to do a few more steps. You've got to sign the data for your zone before it actually gets loaded into the authoritative servers for that zone. The recursive server or end application, we hope at some point in time, but the recursive server itself needs to have the root key and do the validation, so that when the requests are made and the answers come back, you can actually do the validation itself. And for most validating name servers, certainly the open source products, it can be turned on by simply setting one configuration switch the proper way, that's it, that's all it takes to do it.

Now, in summary, the general concept of activities that run their own DNS, the DNS is very important to them. They are going to want to do their own DNSSEC way, their own DNSSEC activities, to make sure that it is run as well and as accurately as their DNS. If an activity has outsourced their DNS operation, they're probably going to want to also outsource the DNSSEC activities. And in some cases, this is getting, it is getting easier.

Many providers of external service of DNS have not, in the past, offered DNSSEC. So, I urge activities to, if they find that their service provider, if you've outsourced it, doesn't do DNSSEC, ask them to. And if they don't, I'm -- not many people will do this, but some of us have, myself included, if they won't find a server who will and change who you're giving your money to, to provide DNS service, so that they'll do DNSSEC.

So, here's sort of our summary slide. These are the sponsoring organizations for this activity, this gathering, this afternoon, come on back up, Dan. And the rest of the time we have really open for discussion questions, answers. And folks, please, come on up and we'll get some questions, I hope.

DAN YORK: So, yeah. If you guys want to come up and grab a microphone here, we've got these are supposed to be -- Okay, yeah, these should be -- Come on up. So, who's got questions? You've seen this all. Anybody? Come on, somebody must.

Kathy's here, oh, Andrew is going to walk around, Dr. Evil. Somebody must have a question for Dr. Evil. Oh, okay, over here, good, somebody. I was afraid I was going to have to start making jokes and that could be painful. Look at Warren there. Okay, go ahead.

ROCIO DE LA FUENTE: Okay, thank you very much for the representation and the presentation, too. I am Rocio de la Fuente, I'm an ICANN66 fellow and I just want to clarify if I understood correctly, that the signing it follows that here are key of the DNS, so if the TLDs do not sign, my domain I register, doesn't have or there is any way to have DNSSEC right?

DAN YORK: Yes. Do one of you...? Okay, so the answer is, I mean, you could sign your domain, you could do the things there but it won't roll up in in the chain of trust so that the TLD, so somebody that’s going to validate it would not be able to confirm all the way back up to the root that it was there. So yes, generally for DNSSEC to work, you need to have your TLD signed.

WES HARDAKER: And you really need to have, ideally, everything signed. So, DNSSEC will protect you from the root down, as far as something is signed. Most of the TLDs today are signed and I think there'll be graphs at the DNSSEC workshop that will show that.

There are over 10 million signed domains, you know, like, end domains like bigbank.com, which probably actually exists and is probably not signed. But you have to be able to validate the entire tree. That being said, even if you can't, even validating down to .com is better than nothing if big bank itself, you know, if there's not a connection below that.

DAN YORK: But to Wes’s point on Wednesday, if you come to the DNSSEC workshop, we’ll have a couple of charts that show some of the different areas that are out there, and we produce some maps, and in many parts, but I don't know which. What country are you from?

Argentina? Okay. Isn't that .ar? Okay, he's checking. Go ahead, back there.

YAZID AKANHO: Hi, my name is Yazid Akanho, I'm from Benin, ICANN66 fellow. Thanks for the presentation and I will say the movie also, it helps us to really understand. I have two questions, actually. The first one is, why deploying DNSSEC is -- I don't know the right word to use, but the deployment is quite slow. Why? Are there technical reasons? Political reasons? Just, why?

The second question, I've been told about the DNSSEC roadshow program, is it dead or is it…? What is the next step of the DNSSEC roadshow program?

And my last question is, to have more explanation on the infrastructure to generate the keys for DNSSEC. I've been told also that there is a separate infrastructure that needs to be maintained in secret, also. Can you explain a little? Thank you.

DAN YORK: Sure. So, deployment challenges, the DNSSEC roadshow, and the information about how to do the signing etc., do I have that correct? Okay. Anybody want to take? Take one of them?

WARREN KUMARI: I'll answer some of them. So, I quickly checked, .ar is signed, so the Argentine... Okay, cool. And for the deployment stuff, yes, DNSSEC hasn't been deployed quite as quickly as it could have been. But some interesting statistics, we're in Canada at the moment, 13.3% of requests are validated within Canada, 25% in the US, 19% in Greenland, 14% in Russia.

So, you know, it's not as widely deployed, it's not universally deployed, but the deployment is actually picking up, and the majority, not quite the majority, but a significant amount of requests are currently being validated and the huge majority of TLDs are signed. Part of the new gTLD contract requires that the new gTLDs are all signed and most of the majority of ccTLDs are signed as well at this point.

DAN YORK: Go ahead, Russ.

WES HARDAKER: If you want to track, you know, things, sort of, daily, my colleague -- Victor, thank you, I was blanking on his name, he and I have a website that actually we update on a daily basis called stats.dnssec-tools.org. And so, that will show you, and if you go look at the graph, you'll see it's continually been going up since 2011. Sometimes there's, you know, gigantic jumps.

There was one, actually, just one the other day because one.com, which is a provider, suddenly signed a bunch of stuff under the .dk domain. So, there's these huge jumps, and really, in order to get deployment, we need more of those, we need giant companies just to do it by default, because the most of the domains that are in use out in the world aren't run by each individual person, it's run by these, you know, companies that are doing DNS hosting.

And traditionally, there's been lots of big jumps, Sweden, being one of the first ones, and there's, in the Czech Republic as well, there's been giant incentives to push people to sign it. The financial incentives, actually, making registration cheaper, has actually greatly pushed signing within particular country codes. For example, to go up.

DAN YORK: Russ, did you want to go ahead?

RUSS MUNDY: Yeah, I'd like to just, maybe, follow up to what Wes was just saying. There's a lot of different incentives that have been used by various organizations to encourage people to do DNSSEC. One of the areas that has helped a great deal is that most of the large publicly available DNS resolver that you see, with four numbers the same, is a pretty common thing. Most all of them are now doing DNSSEC validation.

One of the things, that some of us that have been working in this space have done for quite a while, is we've wanted to see validation actually moved to the end application. And the example that's included in this briefing is where we've had the hijack where Steve Cropper was saying, "DNSSEC won't solve world hunger," that validation itself was done in the browser itself.

And so, as you go and have your interactions and discussion with people, keep in mind that the closer that the validation of your DNS information is done to the end user, the more security you have put into the system itself. So, encourage people to think about going beyond, even the large caching public resolvers, and think about doing it in applications. Now, there was one other question. Yeah.

DAN YORK: So, let me just, on that particular thing, too, part of the deployment challenge is, that as this picture shows, there's actually two parts, right? Everybody who signs and who has a domain needs to sign it. And that's one part. So, it's a signing side, okay. And now, some of that, as Russ mentioned, some of that can be automated; we have any number of the tools that are out there. And if you go and talk to any of the DNS hosting providers out here, some of them can make it super easy.

Some people have a checkbox, you know, boom, now your domain is signed. Some of that is easy, but then the other part is, that you've got to be checking, you've got to be validating that. And as Russ mentioned, sometimes that's just unchecking or removing like a comment line in a configuration file, and now, all of a sudden, you're able to start validating.

But part of what happened, for a long time, was that we had this kind of chicken and egg kind of problem, as we would say in the US, in terms of -- some of the network operators, the ISPs, like Warren was playing, who run DNSSEC validation, they were saying, “We're not going to turn on validation because there aren't enough signed domains.”

So, the operators were saying, “Hey, we're not going to do this because there’s not enough signed domains.” And some of the big hosting providers were saying, “Well, we're not going to sign our domains, because there aren't enough people validating.” So, it was a little bit of people just, kind of, pausing and saying this.

Now today, a lot of that has been overcome, because as Wes said, there's real deployments out here, there's very large, you know, people who are doing recursive resolving. And if you look at some of the big public DNS servers, folks like the Google Public DNS, Cloudflare, Quad Nine, some of those, they're all doing DNSSEC validation.

So, the large resolvers are doing, that large ISPs, you know, are doing it, Comcast here in North America with its 20 million customers that are -- it does all of it through DNSSEC validation. So that argument that slowed down deployment for a while, has now been overcome, but it's still going on there. I know you had two other parts, Fred, did you want to…? Yeah, it's on.

FRED BAKER: So, I wanted to ask Russ a question. Do you know of specific browsers that support DNSSEC validation? What browser -- I only have four browsers on my laptop. What should I be using?

RUSS MUNDY: Well, unfortunately, there is not an available browser that has built in DNSSEC validation. Warren, do you know of one? We did have one and support it for a while, but it's no longer supportable.

WARREN KUMARI: Actually, hang on a second. I think what you're talking about is that's doing DANE validation.

DAN YORK: No, no.

WARREN KUMARI: So, I mean, all the browsers, the browsers rely on the system resolver. If your computer's doing DNSSEC validation. The resolver at the browser is largely just relying on what the system resolver does. So, if you've enabled DNSSEC validation on whatever resolver your computer points at, you get the DNSSEC validation part for free. And I think Wes is going to try and shout at me now.

WES HARDAKER: Not at all. I would never shout at you.

FRED BAKER: Okay. You just told me as a user, I need on my Mac, on your Windows machine, on your Linux machine, I need to go do something.

WES HARDAKER: So, we'll rat hole it as something very technical or very harder to describe, but there's elements that, where validation can happen. Right now, today, applications, which includes web browsers and email readers and anything else that accesses the network, typically don't do the validation themselves. Like the skit, a minute ago, I, Joe User, did not actually check those certificates myself, I trusted my ISP to do that for me. And it actually…

FRED BAKER: Joe User, you terrible person.

WES HARDAKER: I am a terrible person. So, I actually have put validation code into… In fact, the net-snmp package, that Russ was talking about a bit ago, we actually have validation code in that open source package to actually check it in the application. Very few applications actually do that. There's one, one of the biggest, if you go to the stats page I was talking about earlier.

One of the biggest motivations for people signing and deploying right now is that it's one of the only ways to -- it’s really the best way to secure email between servers. So that, actually, is ramping up very, very quickly. It's not all of DNSSEC, but if you look at the ramp up of DANE, which is the technology that signs email conversations between servers, that's actually ramping up quite quickly, and that's done at least near the application, if not in it.

DAN YORK: Okay, Warren. You had a…

WARREN KUMARI: Fred, you said, as a user, you heard you had to do something. As a user, you should make sure that your ISP’s resolvers are validating, you can ask them. Or use one of the, you know, if they don't, you can choose one of the large public resolvers, you know, 111199998888, one of those because all of those validation.

So, if you want DNSSEC protection, use your ISP’s one if they validate, if they do not, use one of the other ones. There's a website, internet.nl, if you browse to that, it's got a thing which will actually check if the recurrent resolvers you're using do validation. And so, that way you can tell if your ISP’s do or not.

DAN YORK: I want to come back to Yazid’s question, but also, I would say, Fred, as far as web browsers go, the other thing is if we, at the risk of rat holing further, but let's just leave it for Wednesday. But things that start doing DNS over HTTPS, as browsers are looking at, and doing those things, many of those endpoints that are doing, that are DOH servers, are also doing DNSSEC validation. So, your browser might actually be doing that if it starts to go down that path, but let's not go to DOH right now.

Let's come back to Yazid’s question, because he's been standing there very patiently and I'm sorry if I mispronounced your name.

YAZID AKANHO: Yazid is my name. Okay, thank you. Thanks to have clarified the resolver’s validation and the zone signature, which are two separate things, as I understand. Two years back, in my country Benin, we were surprised when we noticed that 80% of the request DNSSEC validated by the resolvers. Why? Because some ISPs were using public resolvers.

DAN YORK: Yes.

YAZID AKANHO: And this is completely different to the zone signing, that's why I was asking. Where is the program of DNSSEC roadshow?

DAN YORK: Yes. So, and you're absolutely right, and that's -- On some of the statistics, I don't know, Wes, of yours, but I know Jeff Houston's APNIC stats will show that there are some countries that have extremely high levels of DNSSEC validation going on. And when you explore it, it's because some of those ISPs, in their country, have gone and they're just using public DNS servers. They're not running their own resolvers, they're using, you know, 8.8.8, 1.1, 9.9, whatever, one of the different public resolvers that are out there.

As far as the ICANN roadshow goes, I don't know. We're going to have to get back to you around that because we're not involved with that direct program. So, we'll need to get back to you around that. So, Yazid, just give us, one of us, your name and we can get back to you about that.

Regarding the documentation question around that, I can also, find me, could I can get you your number? The Internet Society published some information on our Deploy 360 part of our website, ICANN has published some information, there's a number of different resources that are out there that talk about the details. And many of the authoritative server companies, ISC, nlnet labs, some of the others, they have gone through and created their own documentation about how to do this. So, there are some good links out there. Other questions? Yes, gentleman there.

UNKNOWN SPEAKER: Thank you. At the risk of being maybe a little off topic, I was wondering how DNSSEC is related to the sig zero pseudo section, in a response.

WES HARDAKER: Not at all, actually. Those are those are different. DNSSEC is designed to protect a set of data and make it verifiable so that no matter how it gets to you, you'll understand it. Sig zero and TSIG is another technology within the DNS for securing things, but they only really secure a connection, not the data itself as it, no matter what path that takes. They're different technologies.

DAN YORK: Yeah, go ahead.

WARREN KUMARI: And sort of, slightly, following on from that, Wes said, you know, DNSSEC allows you to validate the information no matter about how it gets you. One of the nice things that, you know, leads on from that is, a number of people are now actually just downloading the entire root zone into their resolver, because it's all signed.

And so, you can just validate it within your resolver and you don't need to send queries to the root. That's sort of one of the nice things that having a sign zone does, is, in certain situations, you can just, you know, not deal with answering the queries, you can just suck in the entire zone file or let someone else do it.

UNKNOWN SPEAKER: Is that with the transfer request, or do you get the whole zone file?

WARREN KUMARI: So, many of the root server letters, including be B -- B, and F, and I can't remember which others, let you just do a transfer request, AXFR. If you're interested in doing more with this, it's called, local root is one of the names, it's RFC 7706, has information on it, and there's going to be a new version of that soon. But yeah, local root, or hyper local root --

DAN YORK: Hyper local root, yeah.

WARREN KUMARI: -- has a project which allows you to do it through a web page.

WES HARDAKER: Right. Mine is actually called local root and it's localroot.isi.edu and it gives you the configuration you need to actually turn a resolver into a root caching resolver, so everything's pre cached. There's a lot of information on it and hopefully makes it fairly easy for you, if you are a generally knowledgeable administrator; probably not for the end user.

UNKNOWN SPEAKER: And can I just ask one more, more on topic DNSSEC question? If you look at, like, .com, they have maybe a dozen name servers. Do each of them get a unique DNSSEC key for each individual instance, machine, or is it one for the entire TLD?

WARREN KUMARI: So, you actually sign a zone, and so once the zone is signed it can be put on any name server. So, this is especially nice if you operate your own name server, and then you have some other organization who’s, sort of, the slave or the secondary server. You sign your zone, you give them the zone, there's no other keys required. Obviously, you don't need to worry about them becoming malicious or anything.

DAN YORK: Yeah, that's the beauty of the way it works, with that regard, because then, as Warren said, once you have it all signed like that, you can just stop it wherever. It's public key, private key, cryptography. Other questions? They can be generic, they can be stupid, they can be -- Why did DNSSEC just have SEC or something? I don't know. Yes, back there, Yazid.

YAZID AKANHO: Another question. I hear that there are some investigations, or some analyses to change the protocol to generate the public and private keys of the root zone. Where are those discussions and what is next?

DAN YORK: Well, I think some of my colleagues on the table could talk about this, just briefly. You're absolutely right. So, in this signing, when you have the signed, up there on the sign server, you do sign it using a particular cryptographic algorithm, you know. And whether it's RSA or whether it's elliptic curve cryptography, a number of different things, and each of these cryptographic algorithms has different properties, as far as being more secure, more or less crack -- you know, some, some of the original protocols have since been cracked in different ways that people could go and do it.

And so, people upgraded to more secure. Now we're looking at 2,048-bit RSA keys in different ways. We're looking at elliptic curve which are also smaller. So yes, there are different algorithms that are out there. As far as the status at the root, Warren, you look like you want to push your button. No? Okay.

WARREN KUMARI: I guess I'll just make some general comments.

DAN YORK: You were pushing the button right here; your hand was on it. So, I figure…

WARREN KUMARI: I was fiddling with the button. There we go. So, there's a lot of religion around what the best cryptographic protocol is, and if you put, you know, three cryptographers in a room, only one of them will walk out alive, because you'll have stabbed the others and you get into some huge argument about, you know, is RSA better, or elliptic curve, or ED 25519, or various other things. At the moment, there has been some migration from RSA to some newer protocols, but one of the things that some people are starting to talk about is quantum secure protocols.

There's some concern among some cryptographers that quantum computers are going to make the existing crypto stuff not work. There are a bunch of other people who think that this concern is wildly overblown. But it is something that people are starting to look at, and some point, you know, they might, people might start deploying quantum secure protocols.

DAN YORK: I think the answer, those at the root side, there's not an immediate plan to make a protocol change. Oh, Russ, you want to change?

RUSS MUNDY: Well, we're not going to change it, but I wanted to do a promotion for our Wednesday workshop, again. One of the items on the agenda is a presentation by Kim Davies on the plans for the next root KSK rollover.

So, if you're interested in more information about details of when and how and you know how they took all the various inputs, they got from the community, the DNSSEC workshop on Wednesday afternoon has, I think it's a 20 or 25 minute session, where Kim, who's the president of PTI that runs the IANA, will be doing a presentation on their recently released draft plan, which I think was released either Friday or Saturday.

DAN YORK: Hot off the presses. By the way, that workshop will be at 1:30pm next door in 517C and it is several hours' worth of discussions of various different types around DNSSEC, all flavors. Some of it is high level, some of its way down in the weeds, and some of it's in between, and all sorts of things. So, and you'll see a number of us back there doing that. Other questions?

Andrew's standing there with his hand in the air. Somebody's got to help him. Anybody? Anyone? You have a moment of free advice or whatever, otherwise, we're going to ask Warren to start making jokes again. Oh, good. Look at that. Perfect. Just the threat.

UNKNOWN SPEAKER: Alright, this might be a bit of a dumb question, but I just wanted to make something clear in my mind regarding -- it's actually kind of a follow up to the question, Fred asked earlier. So, basically, if I don't have a browser that supports DNSSEC, or like, Outlook, or whatever, does that mean that the section in between my DNS resolver and my client is technically unprotected?

DAN YORK: Yes. So, but now be clear, as Warren was saying too, all of the applications on your device historically have always left the DNS resolution to a little piece of code, the stub resolver in the operating system, which then went out and made queries to the ISP resolver and to do all that kind of things that was there.

And so, if your operating system did not support DNSSEC validation, checking the signatures, then yes, you're at risk of, you know, a Dr. Evil swooping in and providing you with bogus information that could redirect you to another site. Historically, that's been the way it has been, outside of a few things, like examples where people built in, you know, DNSSEC validation into specific browsers, more for test kind of purposes.

This is changing a bit. There's a whole group within the Internet Engineering Task Force, the ITF, looking into the fact that more and more applications are doing DNSSEC. Some of the higher profile stuff we're hearing about with DOH and web browsers is part of that, but other applications are also doing more with DNS validation and stuff in ways that are changing a bit of the architecture of how DNS works and how the internet works in some way. Warren's looking at me like he wants to say something.

WARREN KUMARI: Yeah. Warren thinks you might have actually, or we might all have, oversold the protection some here. So, what actually happens, if you saw it in the skit, the ISP went off and did all the validation and the ISP eventually went back to the user and said, “I validated this. Don't worry, it's good.”

The way DNSSEC actually works is, the validating resolver, the ISP, or public DNS, or whatever, does the validation and then it tells the client that it did it and it should trust it. Basically, it sends a bit saying, “Yes, this is good,” it's all happy. So that does mean that if the packet gets fiddled with on the way back from the resolver to your client, you know, somebody could be doing bad things.

Eventually, it would be nice if your computer did the validation itself, if it didn't trust the ISP, if it went through and did all the cryptographic work itself. And some operating systems you can, sort of, force into doing that. You know, Linux, for example, many of the Debian ones now come with a thing where you can turn on a knob and it will do the validation itself.

Certain people provide software which you can just stick on your machine. There's a piece of software called stubby which will do validation on the computer. But in general, you're largely trusting your ISP or the resolver to have done the right thing for you and to not be lying, and also for your ISP to not be, sort of, tampering with the data on the way back.

UNKNOWN SPEAKER: Yeah, I was-- oh, yeah, if I can just add to my question. I was thinking, more like, you got someone on the local network and maybe he just poisoned the whole thing, and he's, like, filtering, and he just answers the DNS query faster.

DAN YORK: Right, and that's exactly the attack vector that can happen, and this is also why you're seeing a lot of the work happening around DNS privacy, around DNS over TLS, DNS over https, DOH, these things, to look at how do you encrypt the connection from your local, you know, your device to your recursive resolver so that you can have a secure connection there, so that you can't have that person on your local network who’s sending in packets. It's another element of this layers, defense in depth, and layers of DNS protection.

WARREN KUMARI: Yes, sort of following on from that, there's two different attacks. There's somebody on your network, who is poisoning and then giving you wrong answers so that he can force you to go to the wrong place. But there's the equally scary thing of somebody on the network is just watching your packets, and, you know, it doesn't really help if you go to https://alcoholicsanonymous.org, you know, and that all of the content is encrypted.

If people can see that you looked up the name alcoholics anonymous.org, or, you know, gayrights.org or Human Rights Watch, the very fact that you're resolving certain names, the fact that that isn't encrypted potentially is just as damaging as people being able to see the content that you're looking at.

DAN YORK: Russ.

RUSS MUNDY: And this type of thing, that Warren was just describing, sometimes has been called the coffee shop attack, where you walk into your favorite local coffee shop, their WiFi may be encrypted, but that's -- It's freely accessible and anybody in that coffee shop can join that WiFi and they can, in fact, make copies of, or give deceptive answers to your DNS queries.

And so, if you are, if you have a means to protect from your machine to where you trust the information is going to be accurate, then you're going to be less vulnerable to attack. And I know for a fact that this is a doable thing and that there is software available for download on the internet that will let you do it.

DAN YORK: And just to be clear, again, so to just be clear too, DNSSEC is purely about ensuring that you get the correct answers. It's purely about the integrity. What we've been talking about here are extra layers of privacy enhancements and we'll talk about some of those on Wednesday, at our session at 1:30. There'll be some, there's something in there around some of these elements that are part of that. Are you all good? Do you have more?

UNKNOWN SPEAKER: Yes, yes, I'm good. Thank you very much.

DAN YORK: All right, thank you. Kathy tells me we've got something from somebody remote.

KATHY SCHNITT: This question is from Cosi. Can you explain the deal between Firefox and Cloudflare about DNSSEC resolver, I heard it from a previous presentation.

DAN YORK: Well, the DOH. I'm not sure what we -- How much do we want to get into here?

WES HARDAKER: So I can summarize it from a neutral point of view.

DAN YORK: Go ahead, summarize it from a neutral point of view.

WARREN KUMARI: Oh, that’s implying that I'm not.

WES HARDAKER: The problem is, I was the one to give the answer in the previous conversation, and warn you, correct me when I go wrong. How's that? So, there are two -- Let me backtrack and actually answer the previous question, again, really quickly, first.

There are multiple ways to protect the conversation between you and the resolver. Okay, Dr. Evil. There are multiple ways to protect you to the resolver, and the world’s still kind of working that out. And then, the Internet Engineering Task Force in two weeks there’s going to be yet more discussion about it. You can do DNSSEC on your client, you can use something like DOH, you can use something like DOT, there's a number of ways that we're trying to figure out how to protect that, and they all work in different ways.

For the web browsers, the web browsers have decided because they are already well versed in HTTPS, they understand that protocol, they understand how to use it, well, they have really fast libraries that know how to use it. They've decided that they really want to do DNS over HTTPS and they're motivated to do that. They're deploying it in different ways.

And so, the two that I know about, I don't know about plans of the other ones, are Chrome and Firefox. I'll start with Firefox because they sort of went out and announced it first. Firefox decided that they are going to partner with Cloudflare, which is a web proxy and company that does -- they have all sorts of features, and they're also one of the people that stand up a DNSSEC worldwide validating resolver.

They are partnering with Cloudflare to send all of your web DNS requests to Cloudflare, if you use Firefox, and, right now, if you use, if you're in the United States. Their future deployment plans are currently uncertain, but they have backed down to just testing in the United States, this month, and only with Cloudflare at the moment, but they will have a drop-down box that will allow you to pick other providers.

Google, on the other hand, and this is where Warren will correct me when I go wrong, Google, on the other hand is actually going to test your ISP, see does your ISP provide HTTP or HTTPS service for DNS. And if they do, and if they're on a trusted list, they will use DOH to talk to your ISP. If those two things, you know, don't turn out to be true, then they're going to fall back to regular DNS. They're not going to send your traffic to another third party, though, unless that's changed recently.

WARREN KUMARI: As much as it pains me to say that, that's basically all correct. I mean, one thing I'd like to add is, sort of, the Chrome approach. Google believes that, you know, you should continue with, currently, you should continue talking to your current resolver, because it potentially does things for you like malware protection. By talking to your current set of resolvers, they're not changing your resolver, it allows you to get all of your current protections, it allows you potentially look up internal domain names, things like that. And so, that's the sort of Google approach.

DAN YORK: And I think for the remote listener, who asked that question, I think it's important to also understand there's a protocol, DOH, DNS over HTTPS, that was defined by the ITF, RFC 8484. It's a protocol that's basically how to do DNS over an HTTPS connection. There's a protocol called DOH, and a DOH client, which could be a web browser, and that's the primary audience right now, can talk to any DOH server. And it's a way to have an encrypted, secure, private connection between an application and a DNS resolver. So, it's encrypting that connection. So, DOH as a protocol is that.

Now DOH, as it's being initially deployed in these early stages, that's where some of this contention has come in because of these different mechanisms and the different ways that people have asked. So, I just think it's important to understand there's a protocol that works at this privacy layer to ensure that somebody in the coffee shop can't be capturing all of your metadata about all the places that you want to go.

And that's what DOH, and then another protocol called DNS over TLS, which is DOT, those two protocols are designed to help protect the privacy. So, they're there, they increase the level of privacy that we have in that. And some of where the contention gets into is how these are actually being deployed in different ways in these early days. Russ, you wanted to say something, or -- wait. Warren?

WARREN KUMARI: Wes pointed out that I'd forgotten. Full disclosure, I work for Google, you know, who makes Chrome. I meant to disclose that but forgot.

RUSS MUNDY: So for folks that want to see a little bit more, hear a little bit more about this discussion, at ICANN64, I believe it was, there was a high-interest topic session for an hour and a half, two hours, roughly, on DOH, and DOT was mentioned some, but it was a rather lengthy session, and it is recorded, and I'm quite certain is available on the ICANN64 archive website, so you can watch a couple of hours of the ICANN relevant discussion there.

DAN YORK: Other questions? Andrew.

ANDREW MCCONACHIE: I think that was actually ICANN65. Wasn't it the last one, where the DOH session was?

WES HARDAKER: In Marrakesh, yes.

ANDREW MCCONACHIE: Yeah. Yeah. Right.

DAN YORK: Okay, any other?

WES HARDAKER: And I should at least mention, I actually work for the University of Southern California, to disclose where I'm from.

WARREN KUMARI: And I believe that they will be probably more stuff, although I haven't checked the thing on DOH, and DOT, and similar at the DNSSEC workshop.

WES HARDAKER: Yes, we do have a session on DOH on Wednesday.

DAN YORK: Other questions? Yes, up here in the front, a gentleman, right there. And then I saw you, come to you too.

UNKNOWN SPEAKER: I'm Guy, from the US. So, is there a way to do private DNS queries that can't be coffee shopped, that there's no snooping allowed, because the DNS query itself is encrypted in some way?

DAN YORK: Yeah. And this is where both, again, DOH or DOT, those are technologies that let you go and do that, and you can connect from your, well if you want to use those directly, you could do them from your web browser. If you set up either Chrome or Firefox to use, you can set them up now to use DOH and you can tell them which server to connect to. So, you can go and do that now.

You can also go to DNSprivacy.org, right? DNS-privacy.org, where there's a whole series of other different software you can install. You can install something called stubby on your local system, which will go and encrypt all of your queries to certain DOT servers that are out there. So, you can you can do that. You can also run your own DOH or DOT server if you want to. You can run that on your own, in your own place and set that up that way. It's possible to do that.

WARREN KUMARI: And you can also fire up a VPN if, you know, want a quick easy solution now for everything.

DAN YORK: Yes. Yes, you. Other questions? Yes, back there.

ROCIO DE LA FUENTE: My question is in terms of digital literacy. When we talk about educating the user or the registrants, should we explain to them the importance of DNSSEC for their domains, when they register? Because when we talk about the ISPs, the registry, registrars -- not registrar, registers, right? But when we talk about that, that would help the deployment of DNSSEC? What's your opinion on that?

DAN YORK: Well, I think all four of us up here and others here would say, “Absolutely.” We certainly encourage people to include that as part of it, you know, and just say that as you're getting your domain out there and as you're deploying it, it should be signed.

And again, some of the registrars, and I don't know in Argentina, but some of the registrars that are there have gotten to the point, registrars and DNS hosting providers, have gotten to the point where they’ve made DNSSEC as easy as you know, checking a box, or moving a switch, or doing something else.

And that's really, in the ideal world, that's where we want it to go, on the signing side, is where it just becomes something very simple and easy that the end user doesn't even have to really get involved with in some way. But we do encourage people to get out there and get them signed because it ensures from a, from a brand, from a reputation point of view, it ensures that people are going to be getting to the sites that you put into the DNS.

WARREN KUMARI: So, can I disagree slightly?

DAN YORK: Warren can disagree, of course.

WARREN KUMARI: Warren can disagree with anything because he loves arguing. So, I mean, it depends, at which point in the digital literacy cycle it is. I think that we would all say that DNSSEC is a good thing, but is it the most important thing for a new user on the internet? Probably not. Is it the most important thing when somebody registers a domain? It could be, but I mean there's a lot of other security things that are also really important that you need to get right. And so, this fits in a spectrum.

DAN YORK: All right, Warren. That was a good disagreement spectrum. Go ahead.

ROCIO DE LA FUENTE: That's why like, I was thinking about that too. Because when you think about in terms of incentives and, like for us that, we are kind of involving the ICANN and internet governance. If you don't have a technical background, you have to spend time and effort on understanding why DNSSEC is important. So, the registrant or the user, they are thinking about his company or whatever. Like, how do we build a narrative to like, "Okay, this is important. Maybe your domain is going to be a little more expensive, but it has internet or security," right?

DAN YORK: Yeah. This is part of the challenge and quite honestly this is why in many places we've been working with the DNS providers, the DNS hosting providers, or the registrars who may be, often times, the same and encouraging them to either just make this happen, just sign everything, as some DNS hosting providers do, they just sign it by default. Or, to make it easy for people to understand and to do that. And ideally, make it without a cost, although, you know, the business models vary in different places.

Because that's, to your point, Warren, and I will agree with Warren, that in the grand scheme of things of somebody getting online in a new place, this is yet another one of those things they have on their list. But it may not arise, depending on their level of savviness and their ability to work with it, it may not rise to the top.

But it's for that reason, ideally, it's just something that's in the infrastructure. You know, it's being it's being dealt with on those levels. Are you going to disagree with me anymore, Warren? No? Okay, good. He's going to show you. Other questions? We have time for about one or two more. No? Uh, oh, Mr. Levine up here. I say that because I know John well.

JOHN LEVINE: No, this is actually just a commercial.

DAN YORK: A commercial?

JOHN LEVINE: Yeah. A little earlier, a few of you mentioned what quantum cryptography might -- what effect it might have on DNSSEC, and by amazing coincidence, there is a talk on exactly that topic, it's the last talk on Tech Day tomorrow.

DAN YORK: Perfect.

JOHN LEVINE: Yes. The bad news is that the guy giving it as a pompous blowhard, but there's not much you can do about that.

DAN YORK: Okay, well, thank you, John.

WES HARDAKER: We're assuming that's you, John you're okay.

DAN YORK: Oh, alright. Okay. So, John will be giving a talk tomorrow at the end of Tech Day, which, by the way, if you're new, and I see a number of fellows who you said you were new fellows, tomorrow is Tech Day, where there's a number of different sessions that are going on in one of these rooms.

I'm not sure which one, but if you look in the schedule for Tech Day, and there are a lot of different topics ranging from, I guess, quantum cryptography, on this, to DDoS attacks, to other different kinds of things, or various different topics. I haven't looked at the schedule for this for this week, so I don't even know. But anyway, there's a lot of good sessions that are inside of there as well.

WARREN KUMARI: That would be 516C.

DAN YORK: Ooh, listen to that. Perfect. We have found that, which 10:30 is when it starts tomorrow. Anything else? Okay. So, if not, I would say thank you for your attention and also, if you're interested in more, you're welcome to come up and talk to any of us, we'll be around for a few more minutes.

And again, on Wednesday at 1:30 in 517C, the room next door, we will have the DNSSEC workshop, which will cover a range of topics. You can see the agenda if you go up and look at the site on the scheduler, and all of that. So, thank you very much and enjoy your week here at ICANN.

[END OF TRANSCRIPTION]