MARRAKECH – DNSSEC for Everybody: A Beginner's Guide
Sunday, March 06, 2016 – 16:45 to 18:15 WET
ICANN55 | Marrakech, Morocco

JULIE HEDLUND: Welcome, everybody. This is Julie Hedlund from ICANN staff. We will be starting the DNSSEC for Everybody session in just a few minutes, so I encourage you to please come in here to the room and take your seats. Sit up front nice and close so you can enjoy the wonderful skit and see it better.

Then we're going to also have lots of time for questions. We'll have some mics here so that we can get your questions as well. But please, come on out, come on in. We're going to start shortly. Welcome again to the DNSSEC for Everybody Session: A Beginner's Guide.

Welcome, everyone. Please continue to come in the room and find your seats. We're just making sure that everybody gets back in here, and then we'll get started. This is the DNSSEC for Everybody: A Beginner's Guide session, which you see there up in front of you on the screen. Thank you.

DAN YORK: Okay. Good afternoon. How's everyone doing? How many of you have been in this room all day? Yeah. Okay. All right. Well, my name's Dan York, and we're going to talk here about DNSSEC for Everybody. I apologize for the delay. We thought we had video in this room. We're going to be doing a skit, so we told people remotely that they could watch the video, but we turned not to have any video. We were trying to see if we could do something else – to put up an iPhone, doing some kind of video or something – but it didn't work out. So we're just going to proceed and go ahead. All of you who are here in the room get to have that experience.

Oh, I am reminded – we do have translation, so we are going to have to speak slower. I am the worst victim of that. You do not want me speaking French. Once I go beyond "Je m'appelle Dan, je suis américain," I kind of end there. "Pamplemousse." I know that one. I'm trying.

Anyway, how many of you have heard anything about DNS security or DNSSEC? A few people scattered around here. Okay. How many of you have signed a domain with DNSSEC? Okay. How many of you run your own validating resolvers? How many have no clue what a validating resolver is? Good. Okay. You're the ones this is really for.

If you look at the agenda – and you should have received a little handout, a printout, around down here. If you didn't, we have some more floating around. In this session, I'm going to talk a little bit about a view of what could have been the history of DNSSEC and explain a little bit about what makes it special, what is so important about it.

Then we’re going to talk about some of the concepts behind it and give some case examples, some pieces like that. Along the way, you do see people already wearing some T-shirts. We’re going to tell a little story and have a little bit of fun with this as we go through this.

I’m going to begin, I say – oh, I’m pushing the wrong direction. Here we go. I’m confused. So we’re going to take a little journey back into time, and we’re going to the origins of DNSSEC in 5000 B.C. All right? Ready?

This is Ugwina. All right? She lives in a cave on one side of the Grand Canyon. This is Og. He lives in a cave on the other side of the Grand Canyon. It’s a long way for them to go and talk to each other. They have to go all the way down and all the way back up. They don’t get to talk too often about that.

On one of the visits, they notice that the smoke from the fire is going up. They had this idea. They say, “Oh, hey. Wait. We can start using smoke signals and chat from one side to the other.”

But then, one day, the mischievous caveman Kaminsky moves in next door to Og, and he starts sending smoke signals, too. Now poor Ugwina on the other side is very confused. She doesn't know which signals she should be looking at. Which one has the correct information? She doesn't know. She's very confused.

So she sets off to go and climb and try to figure out what could be an answer. Ugwina and Og consult the village elders, one of whom is Caveman Diffie, who has a little idea about what to do.

He runs and he goes into the back of Og's cave. In the back of that cave, he finds this strange blue sand that has only been found in Og's cave.

Now, he runs back out and he throws some of this sand into the fire. The smoke amazingly turns blue. All of a sudden, now Ugwina and Og can chat happily across this by smoke signals because she knows that the blue smoke is the one she wants to pay attention to, and she can ignore all those other attempts that are going on.

In a nutshell, this is what we're doing with DNSSEC. We're providing a special kind of blue smoke, something unique that you can offer that says, "This is the information that I am putting out there." Nobody else has that particular kind of color of smoke. Nobody else has that. Mark's might be red and yours might be green and yours might be orange or whatever. Everybody's got their own color. You each have a unique way of doing that. DNSSEC provides a way to differentiate between information and ensure that you're getting the precise information that's there.

To look at this a little bit more in detail, at a very high level, if you've seen these kind of pictures of DNS, which is DNS itself, we've got the root of that. We've got various different TLDs (top-level domains) that are going on here, and then we have various different second-level domains on here. This is the structure of how it is.

Each of us, whenever we go to a website, when we go to send e-mail, when we do anything like this, we use a resolver. There's a resolver, a DNS resolver, on our smart phone, on our laptop, on anywhere else out there. There's a resolver that is taking the domain name, whether that domain name is google.com or nic.ma or bank.com or whatever. It's taking that domain name, turning it into an IP address, and using that IP address for communication. That's what DNS is doing: just those endless kind of lookups.

Every device has a resolver. The resolver gets that information back and then it holds onto it for a certain period of time. It's got a cache, as it's called, locally. It stores it for a certain period. It might be an hour. It might be a day. It might be a week. It's knowing that the IP address for ICANN, for www.ICANN.org, is whatever. It knows that. It stores that. It holds onto that.

The question that you get into, or the challenge, is that DNS has no security in its native form. Mark over here, sitting her, could come and he could try to get in and tell somebody else what the IP address of www.ICANN.org. This gentleman sitting right back here would believe him because Mark's a little closer, so he could tell that gentleman before I could. There's a wait around here.

This is part of what DNS is. This thing called poisoning up here? We're not actually using poison. That would be bad. What we're really doing is by poisoning – what it means is that, if this gentleman's resolver were to get Mark's information before mine, he would be using that information until it expired. It has a time to live on it; until it expired on that. We'll see this in a moment when we do our little skit.

I'm going to bring up the DNSSEC Players here. We have a group. Yeah. Oh. So we have a little team up here putting on their T-shirts. Oh, and we've got a second microphone, right?

UNIDENTIFIED MALE: Yeah.

UNIDENTIFIED MALE: [inaudible] second mic? There you go.

DAN YORK: Let's check this. Yes. Okay. Wait. Right, okay. I'm not usually the narrator. Okay. You're the ISP. I should introduce our – all right. We'll get this organized. What we're going to do is we're going to do a little skit – would you guys come on yet? Okay. What are we doing? All right. Are we good? All right.

UNIDENTIFIED MALE: Self-organizing.

DAN YORK: Self-organizing. [inaudible]. I should introduce. This is Wes Hardaker, playing Joe User, who's any one of us who's out there surfing the Internet, doing something like this. We have his Internet Service Provider as Jacques Latour there. We have Andrew being the Root Server at the center of all DNS. Warren is the Com Server, and Russ is the Bank Server, as we look like we're getting our props. Are we getting our props together?

UNIDENTIFIED MALE: Yes.

DAN YORK: Okay. All right. The DNS is this massive distributed database in the systems here. So we're going to do this little skit. Now, those of you who know a lot about DNS may know that we're taking a few liberties with how it exactly works. Okay? This is to give a general idea of what's happening around here.

We're going to go through a couple different pieces, and the first part is we're just going to go and do some online banking. Joe User here would like to go and go to his bank. He wants to go and go to www.bigbank.com. Here's what's going to happen in the DNS space.

WES HARDAKER: Well, I need to go pay my electricity bill today because it's about to run out and it needs to be paid, so I'm going to type in the name of my bank into my web browser and go to www.bigbank.com because I want to pay my electricity bill. But I don't actually know where on the Internet that is, so I get to ask my ISP, my Internet Service Provider. Where is that, please?

JACQUES LATOUR: Thank you, Joe User. I'm a recursive name server. I just woke up. I don't know anything, so obviously I got to go look up what bigbank.com is. I'll get back to you with an answer.

The only thing I know is where the root is on the Internet, so I'll go to the root. Hello, Root. I'm looking for www.bigbank.com. Do you know where that is?

ANDREW: I'm sorry. I don't know where www.bigbank.com is. But I know where .com is. It's at 1.1.1.1.

JACQUES LATOUR: Perfect. So I'll go to 1.1.1.1. Thank you. Hello, .com. I'm looking for www.bigbank.com. Do you know where that is?

WARREN KUMARI: Sorry. No, I don't. But I do know where bigbank.com is. That's at 2.2.2.2. You should go and ask him.

JACQUES LATOUR: Oh, thank you. 2.2.2.2. Hello, BigBank. I'm looking for www.bigbank.com. Do you know where that is?

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

JACQUES LATOUR: Ooh. An answer. Thank you. Hey, Joe. The IP address is 2.2.2.3.

WES HARDAKER: Thank you so much. I can go send that $1000 to my electric company now.

DAN YORK: All right. Let's give a round of applause. Now, think about what was happening here. This interaction – Joe User talking to his ISP to resolver – that's happening millions of times a second with everything that we're doing, every time that we're doing a web page, every time that we're doing any kind of interaction with any kind of apps. Anything that has to get an IP address is making that kind of thing.

Now, in the real way this works, the caching side, the ISP would start to have all this information, and the ISP would be able to go right back to Joe User very quickly and say, "Oh, yeah. I know where this is," because Joe User has gone along and cached all this information.

But that doesn't help our story, so we're just eliminating that fact for today to do this.

Now, are we ready with the other element? The other element is ready. Okay. Now we're going to show what would happen here with regular DNS. So DNSSEC has not entered in here at all. This is just the same old plain thing that's happening today.

Joe’s going to do it again, only this time you may see something else happen. Go ahead, Joe.

WES HARDAKER: Oh my gosh. I forgot to pay my water bill. I need to go pay my water bill, so I’m going to go back to www.bigbank.com. But I don’t remember where that is because I don’t keep track of anything. Can you please, ISP, tell me where www.bigbank.com is?

JACQUES LATOUR: Oh, thank you. I just woke up this morning, so I don’t know anything. But I know where the Root is. Hello, Root. I’m looking for bigbank.com. Do you know where that is?

ANDREW: I’m sorry. I don’t know where www.bigbank.com is. But I know where .com is. It’s at 1.1.1.1.

JACQUES LATOUR: Oh, thank you. 1.1.1.1. Hello, .com. I’m looking for bigbank.com. Do you know where they are?

WARREN KUMARI: Oy! I've already told you. I don't know where they are, but bigbank.com is over there: 2.2.2.2.

JACQUES LATOUR: I'm sorry. I'm not very smart. I keep asking questions. Hello, BigBank. I'm looking for www.bigbank.com. Do you know where that is?

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

JACQUES LATOUR: Oh, how cool is that? Thank you very much. Hey, Joe. www.bigbank.com is at 6.6.6.6 IP banking.

WES HARDAKER: Oh, thank you so much. Wow, my water bill's expensive this month. It says I owe a million Swiss francs. But I guess I'll pay it.

DAN YORK: All right. Let's give another round of applause there. Now, you'll notice what happened here was that Jay over here, playing Dr. Evil, performed what we call a man-in-the-middle attack. He jumped in here and he beat Russ to give the right answer. It's about speed. He was the quickest one to get in there, and he got in there. We could have done things like had a denial-of-service attack, where we just kind of push Russ out of the way or something, but somehow Jay got in there quickest and gave the answer.

That's the fundamental attack that we're trying to prevent with DNSSEC. We're trying to prevent somebody from pushing that information in there.

Notice this is all before Joe User has even connected to the site. He hasn't connected and got TLS certificates. He hasn't done anything like that. We're just trying to get Joe to the right site. That's all that we're trying to do.

Okay. So now – okay. They already started here. Here we go. Okay. While I was talking.

To do DNSSEC, to do DNS security, we have to have two parts. There's two parts to it. There's a signing side, which is that the people operating the zones for this information have to put on cryptographic signatures. They have to sign their zone. It involves some software that goes and generates these signatures, which basically says, "This information is totally accurate."

If you think about it like medicine bottles that have that foil on the top, the tamper-proof kind of foil, that basically you can't open the bottle until you tear off that foil to get in there – it says those pills or whatever were packaged by the manufacturer – that's the same kind of thing we're doing with these signatures. We're saying, "This information is what was put in there at the beginning."

So they've gone and signed themselves, and then they pass some information from BigBank up to the TLD, which then passes it up to the root. They're creating a chain of trust here so that an attacker couldn't necessarily pretend there was a signature and do that.

Now, that's the first side. The second side is our ISP over here has to check signatures because if they sign, great. But if he doesn't check, then so what? There's no added security. He's going to be doing what we call validation – DNSSEC validation. He's going to validate the signatures and make sure that they are correct.

Our next act, Act 3 – actually, no. Act 3 we've done here with our signing and shaking and all this. We're all set. Now we're going to go to Act 4 and see how this would play out with DNSSEC coming into the picture.

WES HARDAKER: All right. Today I want to go send a tip to my friend, Dan, who is doing such a great performance I thought I'd sent him an Italian lira. I'm going to go to www.bigbank.com and try and send him, my friend, some money. Can you help me? And I'm now signed up with an ISP that has a validating resolver.

JACQUES LATOUR: Ah, you made a wise decision there. Thank you. So you want to go to bigbank.com?

WES HARDAKER: Yes, please.

JACQUES HARDAKER: Thank you. All right. I don't know anything. I just woke up, so I'll go to the Root again and ask him where www.bigbank.com is.

ANDREW: I'm sorry. I don't know where www.bigbank.com is. But I do know where .com is. Here it's at 1.1.1.1. And let me sign that. There you go.

JACQUES LATOUR: Oh, works out. Good signature. Thank you. It’s valid. I’ll go to .com. Hello, .com. I want to go to www.bigbank.com. Do you know where that is?

WARREN KUMARI: I do actually know where bigbank.com is. I don’t know where www.bigbank.com is. Would you like to know where bigbank.com is? Happy to tell you. It is at 2.2.2.2. Here’s my signature that shows it’s real.

JACQUES LATOUR: Let me check that signature. Let me check you. Yeah, it works out. Perfect. Thank you. Hey, we’re good. All right. Let’s go to bigbank.com. Hello, bigbank.com. I want to go to www.bigbank.com.

RUSS MUNDY: I think so. Yes. It’s at 6.6.6.6.

JACQUES LATOUR: Thank you very much. Thank you. Let me check the signature. Hey! This is wrong! Get out of here! Can they believe that?

UNIDENTIFIED MALE: Thank you, Mr. ISP. I do know where www.bigbank.com is. It is at 2.2.2.3, and I will sign it. There you go.

JACQUES LATOUR: Thank you very much. Let me check the signature. Let me check you. Yeah it matches. Thank you. It's all good.

Well, Joe User, I'm guaranteed the IP address for bigbank.com is 2.2.2.3.

WES HARDAKER: Excellent. Thank you very much. I can go send that lira to my friend, Dan, now. Thank you.

Here you go.

DAN YORK: Awesome. Thank you. And how much is a lira? When can I expect it? Thank you. Let's have a round of applause.

Now, question for you: what did Joe User have to do in this scenario? Did he have to do anything?

UNIDENTIFIED FEMALE: No.

DAN YORK: No. It just worked for him in the background. The ISP – what did the ISP have to do?

UNIDENTIFIED SPEAKERS: [inaudible]

DAN YORK: Validation. Checking the signatures. All that other stuff happened among the name servers that were there. All right? This is, at a simple level, what happens in DNSSEC. Okay? This is what we're trying to do: prevent Dr. Evil from jumping in there and providing that IP address.

Now, it's a little bit more complicated than this. Okay? We're going to talk a bit about what's involved with that. But this is the fundamental process. What do you think? Does that seem good so far? All right?

Let's just review a couple of things on here. Yup, they did this. They did this. We did that. We did the blue thing. We did this, and we're here. Okay.

Just a couple of words that we talk about. We talk about digital signatures, and we talk about keys, and having keys that go along with your information. When you publish your information in DNS, just as you've always done, you also publish a signature.

You generate this. The software is out there that does this. You generate this and you publish that. All that information is stored in DNS.

There's one more piece we didn't really talk about. When the resolver goes to the root and asks for that information and gets back a signature, the resolver also has known about the root's key. They know the key that would be behind all of that.

One of the things you'll hear talked about in the DNSSEC world is an ongoing discussion about the root key rollover, which gets into the changing of that key, something that we'll be talking about more on Wednesday in our technical workshop that we're doing here. There's this chain of trust that goes on from there, and that's what allows the correct thing.

One more point, when the ISP – when Dr. Evil – jumped in there and said, "This is the bad information" and it rejected it, what happened then was the ISP did another query, found the good server, and got that information back there. Or it might have just received the two queries coming back quickly, depending on the timing of that.

All right. We did this. I think I'm going to turn it to Russ to get into a little bit more of the technical details, and then we're going to come back and have a time for questions and answers.

So think about what questions you might want to ask us. We've got a great pool of people here who can help address all that.

Here you go, Russ.

RUSS MUNDY: Thank you, Dan. Okay. See which way is which here. Okay. Good. Well, now I am no longer bigbank.com, but Russ Mundy, here to hopefully help give you a little bit more information about some of the technical parts of DNSSEC and why you should even worry about DNS to begin with.

In reality, as we've done this over time, this part – the "why you should worry about DNS" – is unfortunately becoming simpler because there's more and more attacks that are done that make DNS a starting point or sometimes a very significant part of the attack itself because each and every application – I don't care what application it is on the Internet; there's rare, rare exceptions when you're not using DNS. A few geeky people and a few really geeky applications will still use IP addresses, but for all intents and purposes, you use DNS to do everything on the Internet.

When somebody wants to attack an application, where do you start? Well, one place that they start is the application. But a very common place to also start is DNS itself and changing the

DNS information, just as you saw in the skit itself, because what is it that DNS does in the fundamental sense? It changes the name that human beings really like to use into the numbers that the IP technical underlying infrastructure actually makes use of to move data around the network.

So what you get is you get to the right place or you get to the wrong place if you're attacked with DNS. You as a user have no way to know. That's a very serious problem. That's really the hijack threat that we were talking about: when a DNS substitution or a hijack attack occurs that the user who's asking for the information gets the wrong information, and whatever happens after that, may or may not be visible to the user. But the intent of an attacker is usually to do something bad to the user or bad to the website or other facility, whether it's an e-mail server or something else that he's going to.

One of the things that we've seen in terms of just how broadly available are tools for hijacking the DNS. Unfortunately, there's a lot of them out there, and they're readily available. I don't put the URLs in the slides. That'd make it too easy for people and too broadly broadcasting it.

But in fact, at one point – and the information has been gone from the Internet for a while – there was actually a university professor that I found his coursework that the final project for this computer science course was designing software that did a DNS hijack. So they were teaching that at a college-level course. As far as I could tell, just looking at the syllabus, there was no ethics associated with it. So it was just a software programming exercise, as far as I could tell. It’s unfortunate that people do that, but it’s out there, and there is a lot of software available to do it.

So what are we trying to do with DNSSEC? As you saw in the skit, we’re trying to make sure that the users get the information that is correct and that they then in turn can go to the proper place that they want to get to.

Here’s a slide that gives another illustration of what the skit was showing. This, too, is somewhat abbreviated because I did not include, just because of the business of it, the arrows for starting at the root and going through com. This is just going from one user to effectively www.bigbank.com. So the query goes to the name server for bigbank.com and then that gives him the answer for the www.

When you count the queries – I think I’ve got them numbered on there – yeah, there’s four packet exchanges that have to occur before the user actually gets connected to the web server, which is what the user wants to talk to, anyway. So all these things happen in the background that happen very quickly.

We've got a picture here of a website that's set up to show the user if in fact their DNSSEC is working properly and if it's not. One of the things that we've done here is just put this up as a special example so people can see when they go to this site.

This is, again, another illustration. Dr. Evil is down here in the little yellow circle at the bottom, jumps in, gives the wrong answer, and, as you can see over on the right-hand side – yeah, on the right-hand side – sending people off to the wrong spot.

Now, in this case, we have an example. These are actually screenshots that I took from a real hijack that we did as a demonstration in a meeting similar to this. It was not an ICANN meeting, but it was similar meeting where we actually instrumented the website so that, when you were using DNSSEC to go to the website, you would get the proper content of the website.

When the hijack occurred, you actually would end up having a portion of the page – not the entire page, or not the entire site, but a portion of the page – substituted. You can see that, on the left, with the site that has the DNSSEC checkmark – Comcast shares DNSSEC advice, etc., etc. – and if you see on the right of the picture, further down, there's a story that's actually in front of that, where Steve Crocker is declaring DNSSEC won't solve world hunger. Clearly fictitious, intended to be, but just to make the point.

So when you do a DNS hijack, you may hijack the entire site, or you may hijack a very small, very selected portion of the site, and the user gets the rest of the information from the site itself, depending upon how the hijack itself is executed.

This picture is similar to an illustration that, when you think about filling that page that had several links – this was CNN.com about eight or nine years ago. We checked it again more recently. It's a little more dense than that now. So that's what it takes, the number of DNS queries it takes to fill the browser for the CNN.com home website if you don't have any of the caches filled to begin with. It's well over 100 – well, well over 100. This is close to 200 now. It was about 70 a few years ago.

When you think about it, it's easiest to think about it as the whole website, but it's really not because every large website, every commercial website, has just a ton of links and a ton of DNS lookups. So it can be any one or all of those that gets hijacked.

The importance of all of this and all of the DNS content protection is the DNS content itself. DNSSEC is critical for users to be able to know that they're getting the proper content. But it is no more important than the content itself. In fact, content is the real key here. DNSSEC is put in place to ensure the proper content can be determined by the receivers of DNS queries.

So the crypto-mechanisms you see are not more important than the content. Some people get confused about that fact and they think the crypto is the most important thing. It’s really not. It’s really the content of the DNS zones.

Here’s a couple of short implementation examples. One is just a standard layout of how the user data gets put in. This is entering your content into the authoritative server for a zone. That’s the authoritative server box. The recursive server, who is the ISP – Jacques in our skit here – goes around and asks queries of that in response to Mr. Joe User. So this is another way of just illustrating the way the content is put in and taken out.

What DNSSEC adds is a few more steps that you need to do to make sure that you get the additional DNS information in place and that it gets checked.

What we’re doing here is talking about how difficult or easy it is to get your content and manage your content and manage your DNS, or, if you happen to be a user running a large enterprise operation that includes DNS, what kinds of things you need to do to make sure that they are in place.

I’m not going to go through all these in detail. We want to keep times for questions. If there are questions, please ask them during the question and answer time.

So that’s the main point that I would like to make as far as all of the pieces that are involved in DNS and DNS security: it’s the content of the zone data. It’s the content that counts. That’s what I like to say. It’s the content that makes the difference because you’ve got to put it in properly, you’ve got to manage it properly, and you’ve got to protect it properly with DNSSEC.

In this case, it’s the same set of boxes. The simplest implementation is a zone is signed – we don’t have any pointer? Anyway, the signed data gets put into the authoritative server, and the recursive server is doing validation. The simplest, straightforward implementation that you’ve got, it’s really those two key, critical issues. The zone data gets signed that’s putting data in, and it gets validated by a validating resolver when you get the data out. That’s the simplest straightforward way to get your DNSSEC in place.

In terms of what users might do with respect to implementing specifically for their organization, whatever that organization might be – if you’re a large activity that’s business focuses heavily on DNS (DNS-centered), chances are you have a very highly capable, competent DNS crew already in place.

Organizations like that can normally take and implement DNSSEC themselves. Whatever the pieces are, they can usually do it themselves.

If you're an organization that outsources a lot of its DNS support, then you want to go to those that you're acquiring your support from and ask them to do the DNSSEC implementation of the parts of the DNS that they operate for you.

If they don't, you ought to consider finding someone that does because nothing makes a business move faster than the potential of losing customers. That is an important thing. Ask your vendors if you're doing it yourself. Ask your service providers if you're having someone provide the service for you. Ask for DNSSEC support. That's probably the biggest single message of what any individual can do: ask those that are doing DNS things for them, "Do you have DNSSEC, and if you don't, when are you going to get it? Because I want it and I want it now."

Time for the questions. Dan and I are usually with mics, but we have a panel of experts here. Julie?

JULIE HEDLUND: [inaudible]

RUSS MUNDY: Oh. For the runner mic, absolutely. Yes.

DAN YORK: We've got about a half-an-hour or so. We've got plenty of time. So what do you think? Questions? Yes? I'll come back to you, I guess, since we don't have a mic stand. Here it's fine. We can run around, get some exercise.

JACQUES LATOUR: And they can ask in French and I'll translate.

UNIDENTIFIED FEMALE: Thank you. [inaudible] for Uganda. My question is about the domain name – yes, security, as you've just told us. I keep wondering. One of the ways to secure a domain name is by use of SSL certificates, right? But how come most in my country, most of the government, domain names are hacked into? And how [inaudible] SSL certificates?

DAN YORK: Let's take that apart in a couple different ways. Excellent question because people do ask that. One of the questions they say is, "I've got a TLS (or SSL) certificate, and I'm protected, so I should be safe."

Well, there's a couple of different things that happen. First of all, you've seen here that one area of exposure is this, is getting to the wrong IP address. So one area is DNS hijacking. DNSSEC can protect against that particular threat.

But now you get into, at a higher level, questions around which TLS certificate is being used. Is it the correct one? We have another part of DNSSEC. There's something called DANE – the DANE protocol – which lets you put a TLS certificate into DNS, sign it with DNSSEC, and now when somebody goes to your site, they can know cryptographically that that is the correct TLS certificate to use.

Having said that, of course most browser vendors don't yet implement that. It's a newer thing in some ways around that. But it's used in mail and some other places.

As to why those website are being hacked, there's a whole host of other issues that get into websites that actually happen at a higher level, which is to say the applications. It's oftentimes their websites have problems in the forms, for instance, that would let people go and hijack sites through that, or other ways of breaking into the servers that don't get into [inaudible] TLS because TLS encrypts the connection between the browser and the server. So it provides protection there. DNSSEC is provided protection there, but it doesn't do anything to protect what the people do inside the website. It just makes a secure tunnel, basically, between the browser and that. So they could do all sorts of things inside there, and they could break in through that and other means – oh.

RUSS MUNDY: If you look at the arrows on here, the red arrows indicate the DNS queries, and the green arrow is actually the HTTP/HTTPS query between the browser and the web server. What DNSSEC does is guarantee that you'll get to the proper webserver.

Now, if the webserver itself has had an attack upon it that was successful, that's something that DNSSEC is not able to do anything about. Or if, in fact, the TLS certificate authority was compromised and someone has done something because of the compromise of that certificate authority, that's outside of what DNSSEC can do anything about. So whenever you go to a site that is doing an application kind of functionality, that site still has to operate and function properly. DNSSEC makes sure you get to the correct site, but not that it works properly for you.

UNIDENTIFIED FEMALE: Okay.

RUSS MUNDY: Does that help?

UNIDENTIFIED FEMALE: So [inaudible] security is not guaranteed for –

DAN YORK: No. DNSSEC just guarantees you get to the right IP addresses. TLS guarantees that you're getting an encrypted connection between the client and server. But they're just really protecting the connection of getting there. What actually happens to the server, or on the web browser? If somebody has some malware or something on their server, or on their laptop or something, this just protects the transport and the connection. DNSSEC specifically does the IP addresses and that lookup.

There's a whole host of other things that can cause problems with servers.

UNIDENTIFIED FEMALE: All right.

DAN YORK: Other questions? Over there. Kathy wants to do the running now.

KATHY SCHNITT: I should have worn roller skates.

DAN YORK: I know. Roller skates. That would be good. And if any of you guys want to chime in here, too, Russ and I don't have to talk.

JACQUES LATOUR: That's if you'll let us.

DAN YORK: What? Oh, that's if we let you. Sorry. Go ahead.

UNIDENTIFIED MALE: From the diagrams and the skit, it looks like the DNSSEC needs to be implemented by multiple parties. So the ISP provider needs to support it. The root zone needs to support it. The registry needs to support it, and each website needs to support it. Is that…

DAN YORK: Well…

UNIDENTIFIED MALE: Or I should say each domain name.

DAN YORK: Each domain name, yes. There's a couple of spots in there. Again, there's these two sides. There's the validation side, which is the checking, which ISPs and network operators need to do.

That's fairly easy to do. You can BIND, Unbound, Windows Server. Any of these things that are doing DNC resolution now support DNSSEC validation. So you can go home to your networks today and turn that on.

There's the one caveat that you need to be aware that, if somebody has a bad signature or something, you might block people from going from there. So you have to be aware that, turning it on, you might start protecting people, but that could cause some, if there are problems out there. That's the validation side.

The signing side does involve – yes, the root was signed back in 2010. Most of the generic TLDs and all of the new generic TLDs have all been signed at their top level. Many of the country codes – the ccTLDs – have been signed, although Africa, many of them here, are ones that are missing that signature at that top level. We've been working to help with that. But you need that. And then your registrar needs to support it as well because they have to pass that little signature piece back up to make that work.

So the validation side is relatively straightforward. The signing side? You do need to have those three players in there.

Warren wants to say something – oh, Julie wants to say something.

JULIE HEDLUND: Yeah. I just want to remind people, when asking questions, please state your name and please also state your affiliation. Thank you.

[UNIDENTIFIED MALE]: Yeah. On the ISP or validation side, currently about 20% of DNS requests go through a validating resolver. So there is at least some deployment on that side. It's not quite as much as we would like, but 20% is still a good number.

DAN YORK: Right. And some of the big sites, like Google's public DNS server, do DNSSEC validation by default, so anybody who's using the 8.8.8.8 and [inaudible] IPv6 addresses, that's all be validated by default.

HEATH DIXON: Okay. It's Heath Dixon from Amazon. One other question. You'd mentioned the registrar as well. So is it the registrar or the domain name, or is it both?

DAN YORK: You as a domain name owner may not have to do much, but there's the person who's doing the serving of the DNS records; so the DNS hosting operator, we typically call it, or the DNS operator, which in many cases is also the registrar. But it doesn't have to be.

You folks are a DNS operator, so you are serving out those zones. You have to sign the zones because every time records are changed in DNS, they have to have new signatures, or blocks of records need new signatures.

Okay. Jacques wants to answer. But the key is, the operators have to sign it, and then the registrars – and I know what Jacques doing; okay – and then the registrar has to get this information to pass it up to the registry.

I have a problem with one of my domains is at a registrar that does not support DNS – they don't let me put records in there. So I'm actually moving that to another registrar that does support DNSSEC.

But Jacques wants to tell you about this particular thing, I think.

JACQUES LATOUR: Yes. So you said you're with Amazon, right? I guess some large DNS provide DNS operator. They can sign their zone for themselves or their customers, and the challenge is getting the

DS record to sign the zone through the right registrar to the right registry.

What we're doing now is we're building a new type of interface for DNS operators to self-sign their domain without registrar, or with a registrar. We're working on a new way of making signing bootstrapping domain names easier to address some DNS operator issues.

DAN YORK: Jacques will want to talk to you after this session.

RUSS MUNDY: Thanks for that question. I'd also like to add that in fact the holder of the name, whether or not they are operating any of the DNS services associated with the name, has to be the one that really starts, or if you will, makes the decision: "I want to have this name be DNSSEC-signed."

The details of what has to happen next vary by whatever the particulars of the operation are. Many of us would be happy to go into any amount of detail for any questions that you had afterwards, but I imagine you operate your own DNS resolving and authoritative servers for your enterprise. So it would be my guess that the challenge might be getting the DS record into the registry. There are answers for how that can be done.

HEATH DIXON: Thanks.

DAN YORK: If you didn't realize, any one of us could dive down deep rabbit holes in describing these kinds of things. So if you want to have a deep technical conversation, we'll be glad to.

Anybody else? Come one, somebody else. We've got this pool of people here. They need to answer things.

ADEEL SADIQ: This is Adeel Sadiq from Pakistan. I'm a NextGen participant. Referring to your play, I have to two questions from your play. When the bank was transferring the chain from the bank to User Joe, why can't Dr. Evil perform a man-in-the-middle attack there. First question.

Second question. Why can't Dr. Evil produce that chain of authentication using the bank's IP, even before the bank started that process?

DAN YORK: Does one of our panel want to answer that since I'm being accused of—

WES HARDAKER: Speaking as Joe, I can answer that.

DAN YORK: Okay.

WES HARDAKER: You asked a couple of things. Let me hit the first one first. There is a problem between Joe User and his ISP. Note that that connection was not authenticated. The solution to that is you can actually run a validating resolver on your local device. I run one on my laptop. They're small enough and lightweight enough that I have compiled one and run it on a phone. They're not terribly difficult to put on small device. That is more likely a future step. Some of us are doing it now already.

There's a program called DNSTrigger, which will actually do that for you sort of automatically. It'll try and do it when it can. If you're in a hotel where that doesn't work, which unfortunately that does happen, it'll fall back to using regular DNS. So there is solutions for that coming.

I'm blanking on the second part of your question because I just flew in an hour ago from a very long distance.

[UNIDENTIFIED MALE]: Why can’t Dr. Evil spoof the response?

DAN YORK: Between Big Bank and—

WES HARDAKER: If you remember really quick, in the skit, all of the players exchanged a signature early on, so they agreed ahead of time. When you log into your registrar, for example, and you’re logging in a new domain for example.com, you get to tell your registrar that you need a special record put into com that authenticates your records in example.com. So it’s very tightly linked and Dr. Evil can’t just insert something anywhere.

So it’s not just at the end that he could have tried that attack. Anywhere along the line, from the root down to example.com’s resolvers would have prevented that attack. Does that make sense? I hope.

DAN YORK: Jacques, did you want to say something – oh, okay. You did that. Yeah. Because Dr. Evil could have come in with a packet that had a signature on it. He could do that. But, again, it’s this chain of trust, this global chain of trust between the root to the TLD to the second-level domain, etc., that guarantees that, even if Dr.

Evil came in with that signature, the ISP would say, "Well, you got a signature, but it's not the right signature. It doesn't line up all the way back up to the root."

Something else Wes said as far as – Dr. Evil could have swooped in between the ISP and Joe User. There's actually a working group within the Internet Engineering Task Force, the IETF, called Deprive, which Warren's jumping up because he's the co-chair of it over there, which is working on how do you secure that connection between Joe User and the ISP for DNS so that you could wind up having a secure connection there so that Dr. Evil couldn't swoop in between the ISP and that. So that's one way.

The other way is, as Wes said, Joe User starts running his own validating resolver and just does it all himself another way.

Any other questions? Over here. Yes.

HIBA ELTIGANI: Hiba Eltigani, ICANN Fellow. I just want some brief information about the signing process and the validation; where the certificates are stored, how we are doing the validation, and stuff like that.

DAN YORK: Sure. Anybody else before I – okay. If you want.

WES HARDAKER: When you sign a zone, you have to store keys on your machine. There’s actually a whole document about the best practices on how to do that. You can go look at it. It’s an RFC. I don’t know the number of the top of my head. But you need to store both the certificate and the keys, and then what you actually put into the DNS is only the public portion. So you put your public key in and your parent will put a link to that public key in a special record called a DS record. The private key you do store on your machine, or potentially a separate machine, because you don’t need the private key online. The DNSSEC was designed very carefully so that you could keep your private keys in a very special vault and only pull it out when you need to sign your zone. It never has to be exposed to the real Internet. You just have to transfer the signed records and the public keys to the real DNS.

Some people do keep their private keys online if they’re rapidly updating, if they’re changing things so frequently, or if they’re trying to do live updates for dynamic DNS and stuff. But you don’t have to.

DAN YORK: And there's what are called DNS practice statements, or DPS documents, that are available from all the TLDs that explain what they do.

Now, some like the root zone has a very strong process that goes through in excruciating detail to protect the private keys and to make sure it all works. We have people here who have participated in that, going into vaults and all sorts of different kinds of stuff.

Okay. But for many of the other TLDs, they use other mechanisms that are there. For other domains, for an individual domain, the operator may do it and keep it all in their own systems in some manner. So it all really depends upon the level of risk that you want to have on that.

Now, on the validation side, you're really just inside of your software that's running on your severs. Typically at an ISP, it might be running on the DNS resolvers that are on the edge of the network.

These days, it's as simple as uncommenting out a line in a configuration file that says, "Turn on DNSSEC resolving," and that's it. Now it'll start doing DNSSEC validation all the time. BIND, Unbound: they've all made it very simple to go and just remove the comment mark and just now you're going.

Some of the other ones it might be another step or two in there, but it's very easy to enable that. Then they start doing that validation for every DNS query that they get.

RUSS MUNDY: Also, I'd like to point out that a lot of people look at what they think the most security-critical functionality is going to be done associated with the DNS that they're operating.

As Dan said, the root has a huge amount of security structure around it. They use what are called hardware security modules. Many TLDs also use the hardware security modules so that the only way you can re-sign a zone at the most sensitive level of re-signing a zone is to pull those hardware security modules out the safe, go through a big procedure, and have witnesses. Lots of heavy work.

Other people look and say, "What my zone content is is not being used as sensitively." Okay? The company that I work for is parsons.com. When parsons.com was signed, they went with an external provider because they already had these procedures set up. So each individual activity needs to consider how sensitive the things are that happen with their DNS.

So it's a spectrum of how you handle your keys and your certificates, but it needs to be looked at individually for each activity and then decisions made. But there's lots of help that's available, most of it for free, because there's a ton of examples out on the Internet. There's a ton of practices that people have written down and published openly. So there's a lot of things that you can get information that'll help you when you make those specific decisions because, remember, it's the content and what that content will be used for. That's what counts.

DAN YORK: Jacques wants to weight in. I will just say, as an individual user, I've signed a whole bunch of my domains – oh, go ahead, Jacques, first.

JACQUES LATOUR: The simple answer is, if you use a commercial software that supports DNSSEC, click Yes, and it most likely it will do it right.

DAN YORK: Well, I was going to say, for some of my domains, the DNS operators that I use, one of them has made it that all I do is I check a box that says "Enable DNSSEC," and they take care of everything for me.

In another one, I had to go into another couple of tabs to find the DNSSEC thing. Then I went there and I clicked this and said "Do DNSSEC now," and that was all I had to do. They just take care of changing the keys for me, and they do some of that all automatically.

Now, I also talked about validation. My friend, Paul Wouters over here, who's with Red Hat, pointed out to me that the new BIND, the new Unbound, the newest versions of it, have DNSSEC validation enabled by default. So once you install it, it's just automatically doing DNSSEC validation.

Thank you, Paul. Warren has his hand up over there.

WARREN KUMARI: Yeah. There are also a bunch of DNS providers and CDN providers who are already or will be soon automatically doing DNSSEC for everyone. So this is taking off. If you don't get on the boat now, it's going to leave without you.

DAN YORK: On Wednesday – I'll put in a little plug – there is a DNSSEC workshop happening from 9:00 in the morning until 2:15 in the afternoon. There's an agenda you can see online. There is actually a whole session about getting into some of the software modules and some software signing pieces, etc., that will be going on on there.

We'll have a discussion from one of them, CloudFlare. One of the operators will be there talking about their work at signing large numbers of domains at large scale.

Yes?

UNIDENTIFIED FEMLALE: [inaudible] from Mauritius. So we're speaking about keys, right?

DAN YORK: Yes.

UNIDENTIFIED FEMALE: Do they have an expiry date?

DAN YORK: Yes.

UNIDENTIFIED FEMALE: What is the length of the validity of the keys, and what happens when they expire? Thank you.

DAN YORK: Well, let's answer the second question first. If you think about the fact that if they're checking signatures and a signature suddenly stops being valid, what do you think's going to happen?

Yeah, the validating resolver is going to say it's bad and you can't get there.

Let's tell you a little story. About a year-and-a-half ago now, if my memory works, NASA in the United States, nasa.gov, the space agency, they had signed their domain. All was going along quite well. Comcast is a large operator in the United States. They turned on DNSSEC validation for their 20 million customers in the United States. All of those customers had DNSSEC validation.

Everything was great. All this stuff was going along. Then the folks at NASA had a little slip up. Somebody didn't really pay attention to the exact expiration date of it. There's a defined process. Typically for a key you do it for a year. There's a larger process. There's key signing keys and zone signing keys and stuff that you get into. But let's just say the big key you have to worry about is for a year.

So NASA, somebody wasn't fully paying attention, didn't all work, and the key expired. Well, of a sudden, everybody who was on Comcast's network – and this was actually before Google had done this; it would be even worse today – couldn't get to NASA's website. All right? They couldn't get there. They couldn't see anything. No space pictures, no nothing.

Now, the problem, of course, was that everybody could pull out their mobile phone. They could look on here, and because this was a different network that was not doing DNSSEC validation, they could get to NASA's website on their mobile phone. So all of a sudden – oh, and there's one other factor. This happened on the day – do you remember when there was a big blackout going across on a lot of the web because of the SOPA/PIPA legislation that was happening in the United States?

I see a lot of people shaking their heads. There was a lot of websites that were going to go dark that day in protest of the American government doing those things.

NASA's key expired on that day. So suddenly, people can get to NASA on their mobile phones. They can't get to it on here. "Comcast must be blocking NASA!" Okay? "This is a terrible thing." Social media went nuts. Twitter storms up one and then the other, okay. Comcast's poor customer service people were just like, "What's going on?" because all of this that was happening on here.

Now, it got resolved. Okay? Since that time, we've put measures in place and people have had a lot of discussions. The NASA folks were great because they worked with Comcast to document what had happened and come up with some things. They did a presentation at one of our workshops. It’s probably more than a year-and-a-half. Maybe it’s two years ago or something.

What?

UNIDENTIFIED SPEAKER: 2012.

DAN YORK: Okay. 2012. Three years ago. Okay. All right. A little longer because we’ve been doing this for too long. Anyway, the answer is, if you don’t do it right, then it can cause this kind of outage and this kind of thing.

Now, the good news is that there are systems that are out there now that automate this. There’s well-described best practices. There’s pieces that will do that.

Anyone here from Kenya? Okay. Kenya had an issue with this just last year.

UNIDENTIFIED SPEAKER: [inaudible]

DAN YORK: Yeah. Okay. 2014. So last year, or whatever. In this time, Kenya had a problem with this, too. They had one of their expirations on their TLD, for .ke. All of a sudden the chain of trust broke because the TLD all of a sudden had a bad signature. So everybody who was signed underneath that, great. Awesome. But then when the resolvers went to go try to trace that chain up, they got to .ke and .ke was bad, and so the chain didn't work.

So, yes, you have to make sure that when the keys expire – so signing is not just a simple matter of "Boom. I'm done." You do have to pay attention to the fact that, at some period of time, you've got to redo it.

Now, getting back to Jacques's point, as a consumer, for me, the people I pay to host my domains, I check the box. They take care of that all for me. So I don't have to do anything. But if I were them, I'd have to be paying attention to making sure that those key rollovers worked okay.

UNIDENTIFIED MALE: [inaudible]

DAN YORK: What?

UNIDENTIFIED MALE: Automation and tools.

DAN YORK: Automation and tools. A lot of that has come a long way. There's a DNSSEC Tools Project, which is on the back of some of these, which has some of those tools. The other pieces are happening as well.

I think we have time for maybe one more question or so – oh, we have 15 more minutes. Okay. So any more questions? Yes, back there? Oops. I'll get it.

UNIDENTIFIED FEMALE: [inaudible] from Uganda. Just asking who takes care of those signatures? Is it the domain name server controller, or it's the domain name owner?

DAN YORK: It's the one who's providing the DNS service. The holder of the domain name, or the owner of the domain name – somebody out there, some DNS server, is providing the information. Russ in that picture was doing the BigBank, so he was providing the information for BigBank. So he does the signatures.

You as the owner, if you were the domain holder, you've arranged with him to do it.

Now, you might do it yourself. The gentleman over there from Amazon runs his own servers, so he's doing all that himself. You and your technical team or whatever could run their own servers and do that.

It's whoever operates the servers.

Anyone else? You got a few more minutes. Come on. We can take questions in French, too. We've learned that. If you've got questions in French, Monsieur Jacques will translate them for us, so don't be afraid about that.

WARREN KUMARI: Yeah. Please ask a question in French. It would be fun to watch Dan trying to figure out what it means.

DAN YORK: Now remember, he's French-Canadian, so his French may not be yours. Okay. Here we go.

JACQUES LATOUR: Question in French? [inaudible]

UNIDENTIFIED MALE: As I'm fluent in French, I [inaudible] now. I would like to know that since you have decided that the signature was for the resolution process, I don't understand therefore why, what is the role that is played by the registrar. What is the role of the registrar? Explain to me what, the signature process, is the role of the registrar.

JACQUES LATOUR: The registrars do not have a very important role in DNSSEC. There's no added value to the registrar for the DNSSEC. It is the problem that we have in Canada for .ca. We have 180 domains which are signed, the reason for which is because one registrar in 180 supports DNSSEC. They're not interested. It's a cost added to their operation. It's too expensive.

So we are looking for a good method to sign the domain name without using the registrar. On Wednesday during the DNSSEC Workshop, if you come we will talk about it.

DAN YORK: All right. German speakers, I could help you here, but – oh, there we go.

UNIDENTIFIED MALE: I'm going to carry on in French. I'm from Mali. Does ICANN publish today a list of the registrars who support the DNSSEC for the gTLDs?

JACQUES LATOUR: For the new gTLDs, it is mandatory to support the DNSSEC. For the registrars, DNSSEC for the gTLD – oh.

Is that mandatory now?

UNIDENTIFIED MALE: That's the general rule. Yeah.

JACQUES LATOUR: In general, they should support the DNSSEC, but they don't support it all the time.

UNIDENTIFIED MALE: Is there a list that is published and updated by ICANN?

JACQUES LATOUR: No.

UNIDENTIFIED MALE: I'm going to still speak in French. I'm going to ask a difficult question because the DNSSEC we talked about it in the university. It is a technology which was published about 20 years ago. Actually, 19 years ago. Why is the DNSSEC not deployed everywhere today? Where's it blocked? Why is it not everywhere? Is there a problem somewhere?

JACQUES LATOUR: It is blocked at the registrar level, especially right now. The DNS operators want to sign the domain names, but they're too far from the registries to create the DNSSEC chain. Therefore, the registrars do not support the DNSSEC, and that's where the block is. All the big servers support DNSSEC by default. It's coming, but the big problem lays with the registrars.

DAN YORK: I got a few words of that. All right, over here. Particularly Red Hat. I figured that one out. And Microsoft I think I heard in there, too.

JACQUES LATOUR: And you can put this on Channel [inaudible]

DAN YORK: I know. I should have had that on. We have translation. Go ahead.

UNIDENTIFIED MALE: I am [inaudible]. I am an attorney in Paris, with the bar in Paris. I suppose that in this organization of the security of the DNS, the VeriSign company which provides us with a number of services, this company is a big support; the electronic signature that is used by the legal services all over the world and by technicians in my field.

Do you have relationships with the legal people? Do you have good relationships with these people? In the European Union, they have an allotment of research in security exchanges. There is a big European contract that will be in application in July and a recommendation for using the electronic signature all over Europe when it comes to legal and technical. The European Institute of Telecommunication did the work.

Do you have a relationship with the legal field, with legal experts?

DAN YORK: Sadly in English. You raise an excellent point. I'm not familiar with that particular legislation happening there, but I remember the Internet Society policy people discussing this. So I will need to go back to them and find out a little bit more because you're absolutely right; there's an opportunity there to look at how could DNSSEC be part of that or in some way.

Thank you for that suggestion. That was excellent. We'll note that in there to see what's there.

We have been talking to some people in the content industry – the movie studios; some of the folks like that – around the use of DNSSEC to protect some of their sites, again, looking to make sure people get there. So thank you for that.

Jacques?

JACQUES LATOURL: I'll keep it in English. The discussion was about legal signatures, electronic signatures, like [inaudible] signatures for the legal system, and making a link of that to the DNSSEC or DANE world.

In the future, DANE would be a potential framework for enabling that and the global DNS so that people and signatures potentially can be linked somehow. But I have no clue how or what you will need to do. But potentially it could be an application, looking at DANE. Thank you. [inaudible]

DAN YORK: Any other questions? We have time for maybe one more. Yes, over there?

UNIDENTIFIED MALE: Hello, Olivier. I am from Congo. I would like to know when can we know that the domain name is already signed with DNSSEC? Because we had a workshop on this, and we realized that, in order to know that the domain was name, you had to install a plug-in to see if that site was signed with DNSSEC. I would like to know what stops. Why is it today there are no tools to detect if the DNSSEC has been signed like we do it with the SSL certificates?

DAN YORK: The question is, where is there no [inaudible] answer whether a domain name is signed. There's a plug-in that you can put in that will show you, but why is it not part of that?

Let me ask a question. How many of you pay attention to the green lock in your web browser? Okay. All right. Good. How many of you, when you – yeah, okay. How many of you when you get that warning or something that says the certificate is not correct or something like that just click on through? All right. Yeah.

One of the things that's been found is that most people just kind of ignore – yes, we do see the lock, but if there's a problem with the lock, we just go through because we want to get to the site or something like that. So some of that visual identification that a domain name has a TLS certificate or has been signed has been shown that it doesn't really work.

What's happened in the DNSSEC space was that it happens below that level. If a domain name has been signed and it's good, you'll just see it. If a domain name has been signed and it's bad, you won't get there, or if there's a conflict, if there's an attacker trying to come in there. You get what's called a serve fail in DNS, to get geeky for a moment. You can't get to the site. It's taken below that. So there's no user interaction at all. The user doesn't see it.

Right now, quite honestly, the only way to know that a domain has been signed is to use some other tools, some other websites that are there, that let you see that a site's there.

I think there's some folks who would like to make it easier for you to see if a domain's signed.  There's a browser that Russ' team developed that does that. There's the plug-ins that you mentioned that do that.

There's a kind of a division. Some people would like to show that. Others just say, "Let's just make it secure or not secure." So the answer is, I'm not sure when we'll see that because it's partly a religious war.

RUSS MUNDY: Well, also, as Dan mentioned, studies have shown that the effectiveness of putting a visual indicator up for a user is at best questionable because they usually feel they have to go get to wherever they're going anyway and will tend to work around it or ignore it.

One of the other counterar-guments relative to whether or not DNSSEC is present is a lot of people want it to truly become the ubiquitous default that happens and the only time you should ever need an indicator is if DNSSEC didn't work. So wanting to get to the point of being able to show, "Oh, there's a DNS problem," and just describe it as a DNS problem when there is a DNSSEC failure.

That's one of the reasons we continue to have these educational series and workshops is to encourage people. I love that question. Why don't I see it? Why can't I get more information about it? That's really great. Pass it on outward to the people you work with, to the service providers, to your IT department.

DAN YORK: I know we're running out of time. We have two quick questions left. I will also say while we're doing that, too, if you're interested in more, we do have this workshop on Wednesday, where there'll be a lot more information.

Let's go ahead. Question?

NOMSA MWAYENGA: My name is Nomsa. I'm from Zimbabwe. You mentioned something about African DNS traffic. From your observation, there isn't much DNSSEC happening. Is there a way you're actually trying to build capacity specifically for the – and how?

DAN YORK: The answer to that is that a number of the – once the root of DNS was signed in 2010, a lot of other TLDs around the world started to sign that. On Wednesday morning, I'll put up a map that shows the deployment. But you can actually get to this. I'll tell you how in a minute.

A lot of African ccTLDs still have not signed. Now, there's two things that are happening that are changing that. A gentleman back here mentioned the workshop that was going on. ICANN, along with the Internet Society (ISOC), along with the Network Startup Resource Center (NSRC) have been going around, working at a lot of different countries, to go and work with typically the registry network operators in the area and others to bring about DNSSEC signing.

Anybody here been to one of those workshops? Mark has. Yeah. Okay. Mark's been doing them. The gentleman over here has. Okay. The workshops have been going on to help build that.

What place you can find out more is if you go to dnssec-africa.org. It's a site that's being run by Alain Aina. I don't know if you know Alain, but he's working on that site. There's a place there that shows DNS statistics, which will show which countries have signed and which have not, and also gives links to find out more about how to get more connected.

Also, on the back of this sheet – and if you didn't get one, there's a few more up here, and we can get you more about this – on the back of this sheet, there's a list of resources that are here, including information from the Internet Society Deploy 360 Programme, the DNSSEC Tools Project – a number of other different pieces of information that's out there. So some of these are places where you can start as well.

This I realize does not have dnssec-africa because I actually just learned about it earlier this week. I didn't realize Alain had done as much as he's doing there with it. But it's good stuff there.

[Is that an] answer? Okay. Gentleman over here?

UNIDENTIFIED MALE: HI. I'm [inaudible] from Morocco. Can we just say that one of the reasons that DNSSEC is very slow in its deployment is because there are other tools that make it easier to secure protectors from hijacking?

Also, that having some remote hijacking is very difficult.

DAN YORK: The answer to that is that, actually, DNSSEC deployment's been moving along at a – we'd certainly always like it to be quicker, but as Warren said, we're about 20% validation, higher in some areas. We have some good signatures happening in some places.

Part of the issue is that DNSSEC only solves one part of the puzzle, right? It's one piece of that. On the TLS side, there's a number of other technologies that are out there, like certificate pinning, some of the other pieces that are being used there. But they, again, solve another layer of the puzzle. So DNSSEC solves its puzzle very nicely, solves its piece there. So it all fits together and complements each other.

UNIDENTIFIED MALE: As I saw, that DNSSEC protects us from direct hijacking, like in Alain's environment and so on, so there are other ways we can protect ourselves in these types of environments. So is this the reason that makes DNSSEC deployment very slow?

DAN YORK: I'm not quite sure. We could talk a little bit more afterwards, maybe to understand a bit about that. There are certainly other methods of hijacking sites, and there are other protection mechanisms that are there.

DNSSEC, again, solves that DNS issue, making sure that people are getting the IP addresses you put in there. But that's one type of hijack. But there's other hijacks, too.

UNIDENTIFIED MALE: Okay. Because we should go through a man-in-the-middle attack to poison another's cache. So we can protect from this using the [inaudible] or other mechanisms.

DAN YORK: Did you want to say something? Nah? Well, I'd say that there are certainly – DNSSEC is just one part of a whole defense in depth. We talk about it here because we're at ICANN talking about DNS. So for us, securing the DNS is what we're here to do. In our view, we need DNSSEC to bring us to an open, trusted Internet that truly lets all of us have the opportunities that we want. So this is a tool we have to go and do that.

Oh, Warren does want to say something now.

WARREN KUMARI: Yes. I guess one thing worth mentioning is many of the other sort of man-of-the-middle type attacks require you to be local to the user – DHCP poisoning and stuff like that, ARP spoofing. You have to be local to the user or on their network path.

For DNS-type poisoning, if you do not have DNSSEC, you can do it from a much, much wider range of places. You can do it from anywhere on the Internet, and you can also affect a large number of users. So the scale of the attack is much larger.

You need many different sets of protections. DNSSEC provides one, but it provides a very useful one.

DAN YORK: Also, many of the other mechanisms are called trust on first use. They need to be able to be sure they connect to the right place to begin. DNSSEC helps provide that trust that you're getting to the right place at the right time.

With that, I do want to wrap up because I know we're right about the time, it's here. I want to encourage you all again: the resources are on the back of here. For those who want to dive in or learn more, there is the DNSSEC Workshop on Wednesday. I'll mention that the beginning of it may be of interest for some of you because it's talking about DNSSEC applications and usage across Africa. There's a panel that will have Mark. It'll have a couple other folks. It'll have Alain talking about the work he's been doing and some others. That part may be of particular interest to some of you.

The agenda is posted on the website. It's the Wednesday DNSSEC Workshop. You can figure out which parts of that you'd like to attend to. We try to keep it running right on time so you can know which times to get there.

I'd like you to join me in a round of applause thanking everybody up here for this. We'll be around for a few more minutes if you'd like to talk to us. Thank you.

JACQUES LATOUR: Merci.

**[END OF TRANSCRIPTION]**