COPENHAGEN – DNSSEC for Everybody: A Beginner's Guide
Sunday, March 12, 2017 – 17:00 to 18:30 CET
ICANN58 | Copenhagen, Denmark

WES HARDAKER: How many people have not seen this skit before? Excellent. You're here for the right reasons. This is all about why we have DNSSEC, and what it is actually doing for you and how it's protecting your infrastructure and your domain data when you have used DNSSEC to sign your zone. So, we're going to get into all the details about that. But first, a short story.

Some people claim that the origins of DNSSEC date back to 5,000 B.C. I'm a little skeptical myself, but we'll run with it. We're going to have a couple of characters be introduced into this cast. The first one is Ugwina. This is Ugwina. She lives in a cave on the edge of the Grand Canyon.

This is Og. He also lives in a cave, but he's on the other side of the Grand Canyon, completely across he cliff so that they can't actually communicate that well. It's a long way down and a long way around, and Ugwina and Og don't really get to talk very often.

On one of their rare visits, they notice smoke coming from Og's fire. They soon realize that they can use this smoke to chat. So, as we go throughout the rest of this example, the smoke is like

DNS. You have this distant client that's asking questions and you can answer with these smoke signals.

Until one day, mischievous caveman Kaminsky – Kaminsky was the person that found one big hole in the DNS that allows spoofing; we'll get to that in a minute – moves in next door to Og and starts sending alternate smoke signals.

Now Ugwina is really confused. She sees these two signals and she doesn't know which one to believe. One says, "I really like you, Ugwina." And the other one says, "I really don't like you, Ugwina." Should she feel happy or sad?

Ugwina sets off down the canyon to try to start sorting out this whole mess. Ugwina and Og consult the wise village elders. Caveman Diffie – from Diffie-Hellman cryptography fame – thinks that he might have a really good idea. In a flash, he jumps up and runs into the back of Og's cave. There he finds a pile of magic blue powder that only exists in the back of Og's cave, not anywhere else.

He runs out and throws it on the fire, and poof! All of a sudden, all the smoke turns blue. He thinks this can help them because now, when distant Ugwina and Og wanted to communicate, she only has to believe the blue smoke. She knows which one is Og and which one is the evil Kaminsky.

So, that's the short introduction to DNSSEC from the 5,000 B.C. era. We're going to see how that actually works with real modern DNS traffic as the evening goes on.

If you're not really familiar with DNS, the high-level concept is that there's this tree-like structure. It's sort of an inverse tree, and what happens is that the DNS resolvers that are answering queries for you start off at the top – they start off at the very root – and the root knows where the things right below them are, like com and uk and things like that.

Each of those has stuff underneath them. Bigbank.com is underneath com. And com knows where bigbank is, but the root doesn't know where bigbank is. So, it's a tree-like structure, and well get a better view of this again in a minute.

As I said, the resolver knows where the root-zone is and it traverses that whole tree trying to find the answer for you when you go into your web browser and type in a domain name. Every level simply points at the next level until the question has finally been answered.

One benefit is that the resolver actually caches this information to make it faster. It knows the next time you ask for bigbank.com, it can answer immediately without actually going back and starting the whole process over again.

The problem is, with the past [and] the high-level concept of DNS – and this really should say "without DNSSEC" because DNSSEC solves all these problems – there is no security. There's no guarantee, just like the blue smoke versus the white smoke. Unless you have the blue smoke, you can't actually figure out which answer is correct. So, names are easily spoofed and caches are poisoned as well. So, once you get a bad answer into a cache, that resolver is going to keep telling you the bad answer as long as it keeps that in its cache.

To really illustrate this point, we're going to do a little skit for you. So, I'd like my skit actors to please stand up. I'll introduce their roles in a minute. You can line up over here, folks.

Unfortunately, due to some missing personnel and some illnesses, I'm going to actually play a role in the skit and try to narrate this at the same time. Excuse me for any mistakes I make along the way.

I'm going to start off and I'm going to be Joe User. I'm going to be the user on the Internet that wants to do some banking today.

You wouldn't believe how many times we've worn these shirts. All right.

So, I'm going to be Joe User. Let me give you the quick introductions. This is Mr. ISP. He is who, when you say, "I want to go to this webpage," you talk to him first if you're a user like me.

Bigbank.com knows all the information for the bank.

Com knows where bank is – and, yes, you guys should switch.

The root is where the source of everything starts. So, the root knows where to find com and all the rest of the TLDs.

With that, we will begin.

I'm going to go to my computer. I need to do some banking today. I just want to check my balance, so I'm going to log into my machine and say, "I need to go to bigbank.com," and then I have to wait for DNS to finish before it even starts.

WARREN KUMARI/ISP: So, you want to go to bigbank?

WES HARDAKER/JOE USER: I do.

WARREN KUMARI/ISP: Okay.

Hello, root. My user would like to go to www.bigbank.com. Where is that, please?

KATHY SCHNITT/ROOT: Well, hi, ISP. How are you doing?

WARREN KUMARI/ISP: Good.

KATHY SCHNITT/ROOT: Good. I really don't know where bigbank.com is, but I can tell you where .com is. .com is at 1.1.1.1.

WARREN KUMARI/ISP: Cool, thanks.

Hey, .com. I'm an ISP. One of my users wants to go to www.bigbank.com. Where is that, please?

JACQUES LATOUR/.COM: Oh, I'm sorry. I don't know where that is. But I know that bigbank is at 2.2.2.

WARREN KUMARI/ISP: Cool. Thank you.

Hey, bigbank. One of my users wants to come visit you. Where is www.bigbank.com?

[IRWIN LANSING]/BIG BANK: Just give me a second. I have to look at up…bigbank.com? Well, it's at 2.2.2.3.

WARREN KUMARI/ISP: Cool. Thanks. My user is going to be really happy.

Here you go, user: 2.2.2.3.

WES HARDAKER/JOE USER: Perfect.

All right. So now my web browser goes off and I can check my balance and find out I have a million dollars. So, I'm going to go away and think for a bit about how I can spend that money.

As you can see, that's how the DNS works without any sort of problems.

As you remember, Ugwina the resolver is actually chatting with Og the server. So, we have Ugwina over here – Warren – and the server is over there. Before, she was confused – until they figured out this whole magic smoke kind of thing.

Now we're going to see what happens when bad things happen and how DNSSEC actually fixes it.

Imagine if you will that there are actually two bigbanks out there willing to give you answers – one good one and one bad one. The problem with DNS is that you believe whichever answer you get back first. So, whichever one you hear is the one you're going to believe.

DNSSEC actually fixes this by providing the magic blue smoke cryptography signatures to ensure that all of the information is correct and it came from the right place. The keys in the signatures are all used to make sure that everything stored in the DNS is perfect and has not been modified since its publisher created it, no matter where it came from. That could be in the cache. It could be from the authoritative servers. It could be from anywhere.

DNS is a lookup system, so the keys can be looked up like anything else. The cryptographic keys are actually stored in the DNS as well.

The resolver only needs to know the key of one server – Kathy, raise your hand – the root. If you know that key, you can find the keys to everything else in the system. So, you only have to memorize one public key and everything else works. And it builds a chain of trust. Each level signs the next key for the next level until the chain is complete, and you can get all the way down the tree to find a secured answer.

What that last slide was trying to show you is that you can see the checkmark on the bottom. It provides little checkboxes to make sure that you got from the top, all the way to the bottom, to the right place. You know that the red one is actually lying to you.

Let's go back to our skit. [inaudible] the other one first. I'm going to try and log in and do some more banking.

Let's see. I've decided with my million dollars that I'm going to spend $1,000 on a new computer that I can sign my data with.

WARREN KUMARI/ISP: Wow. If you've got a million dollars, we're going to have to start charging you more for Internet access. But I'll go try and look that up.

Hello, root. One of my users wants to reach www.bigbank.com. Can you tell me where that is?

KATHY SCHNITT/ROOT: Hi, ISP, again.

WARREN KUMARI/ISP: Hi.

KATHY SCHNITT/ROOT: We're becoming pretty good friends. I really don't know where bigbank.com is.

WARREN KUMARI/ISP: You're not very good.

KATHY SCHNITT/ROOT: No. I pretty much suck. But I do know where .com is. It's at 1.1.1.1.

WARREN KUMARI/ISP: Cool.

Hey, .com. One of my users would really like to go to his bank. Can you please tell me where www.bigbank.com is?

JACQUES LATOUR/.COM: Hmm. He seems to have a memory problem. I don't know where bigbank.com is, but I know bigbank is at 2.2.2. I don't know where the website is.

WARREN KUMARI/ISP: I'll go and ask the name servers for bigbank.com. Hello, bigbank. Can you please tell me where www.bigbank.com is?

"DR. EVIL": Oh, yes I can. You can find www.bigbank.com at 6.6.6.6.

WARREN KUMARI/ISP: Cool. Thanks for the quick answer. By the way, you look way better than the old name servers.

6.6.6.6.

WES HARDAKER/JOE USER: Why thank you so much. I appreciate it – hey, where did all my money go?!

So, you can see the problem, right? You believe the first person that actually gives you an answer.

Now we're going to run the exact same scenario again, but with DNSSEC in play.

I'm going to ask my ISP again: where is www.bigbank.com? Mr. ISP?

IRWIN LANSING: Give it to Warren.

WARREN KUMARI: Gimme.

WES HARDAKER: We've rehearsed this. Really.

You need that.

WARREN KUMARI: You need it, too.

WES HARDAKER: I did it.

WARREN KUMARI/ISP: Your turn.

WES HARDAKER/JOE USER: Excuse me, Mr. ISP? Where is www.bigbank.com?

WARREN KUMARI/ISP: I'll go find out for you.

Hi, .com. Remember me? One of my users wants to go to www.bigbank.com. I'm not very good at remembering things. Can you please tell me where that is?

KATHY SCHNITT/ROOT: Your user does too much banking. Well, I don't know where bigbank.com is, but I do know where .com is. He's at 1.1.1.1. But before you go there, I think I probably should sign this.

WARREN KUMARI/ISP: One sec. Yeah, that kind of looks like your signature. Okay. Good. Thank you. I'll believe that.

Hello, .com. One of my users would like to go to www.bigbank.com. Can you please tell me where that is?

JACQUES LATOUR/.COM: Oh, sorry. I don't know where www.bigbank.com is, but I know where bigbank.com is. They're here at 2.2.2.2.

WARREN KUMARI/ISP: Can you please sign that so I can actually believe it?

JACQUES LATOUR/.COM: There you go. All signed.

WARREN KUMARI/ISP: Yeah, that kind of looks reasonable. Okay. Let me go and ask 2.2.2.2.

Hello, 2.2.2.2. Can you please tell me where www.bigbank.com is?

"DR. EVIL": Oh, yes, I can. You can find www.bigbank.com at 6.6.6.6.

WARREN KUMARI/ISP: Awesome – uh, hang on a second. That signature doesn't look right. I'm not believing that.

Hello, bigbank. Can you tell me where www.bigbank.com is?

IRWIN LANSING/BIG BANK: I'd love to see my users, so I'd love to tell you. It's at 2.2.2.3. And look, a green signature.

WARREN KUMARI/ISP: Whoa. That signature matches. I'll trust this one. Thank you.

Here you go, user: 2.2.2.3. And I checked it. You can believe in that.

WES HARDAKER/JOE USER: Well, all my money is still there this time.

All right. So, that's basically how it works. Can we give a round of applause to our actors here?

[applause]

Then we're all going to take off our t-shirts. It'll be entertaining as well.

All right. Hopefully that gives you a high-level concept. If you walked away from the day with just that, it explains what's going on. We're going to go into greater detail and you're going to learn more as the evening goes on, but that's fundamentally how it works. When you sign all of your domains, you end up being able to secure those answers so no "Dr. Evil" can jump in the middle.

First off, here's an example of why you need DNSSEC in a simple guide to getting started.

Why worry about DNS at all? Users think in terms of names. Nobody remembers IP addresses and types them in. We've always used names since, actually, the very beginning of the Internet.

Applications primarily use names, too. When you actually submit something to your web browser, it's not actually just looking up information for the name you've looked up. It's looking at information for images coming through and JavaScript and all sorts of other stuff embedded in your web

pages. We'll see a detailed slide about that a little bit later on as well.

But the Internet actually uses addresses. You don't actually send names around that much, except over DNS. From then on, you're using IP addresses the entire time – be it IPv4 addresses or IPv6 addresses.

DNS actually provides the glue. It translates those names into IP addresses so your software can actually do what it's supposed to do. Proper DNS functions are required by essentially everything. There's almost nothing on the Internet that works without DNS. It's a critical component of the Internet and how it works.

The problem is, of course, that it can be hijacked, as we just saw in the skit. DNS attacks provide a way to divert the applications away by answering faster and answering with wrong information. You believe the very first one that you typically get.

What happens is, users can be redirected to another webpage. They can be redirected to a different IP address that still hosts the same-looking thing. And when you log in with your credentials, you'll find that your user name and password has just been stolen. That's the man-in-the-middle-type attack.

There are multiple hijack tools available. If you actually just go look on the web today, it's not that hard to find some. They've been around for a very long time, and some universities even use it in their coursework, saying, "Hey, demonstrate for me, Mr. Grad Student, how to hijack somebody else's infrastructure."

So, DNSSEC is the answer to this. DNSSEC is the equivalent of the little stickers on the cards. It assures that you're getting to the right place. It proves cryptographically, without a doubt, that you're getting the right data out of the system that was created by the person that owned it.

So, the original zone maintainer created the data and signed it, and no matter how it got distributed – it could be distributed on a piece of paper that I fly across the room – you can check the signatures on it and it will still be valid. It doesn't matter how you get it.

So, the hijack example that we just saw showed what goes wrong. We actually have some other examples of it. This is a pictorial diagram of something similar.

Normal DNS web exchange – I'm not going to go into detail on these – looks like the same sort of things. We have – does it have an actual pointer? Ah, it does. What do you know?

We have an authoritative name server. We have a web server. We have recursive name servers that ISPs use to ask all the questions, and then Joe User down here. So, it's pretty much the same diagram we just saw in the skit. It gets a little more complex the more you think about it because there can be multiple recursive name servers and there could be multiple web servers and multiple authoritative servers. But it's the same type of thing in general.

Uh, oh – that's not good. Oh, there we go. Don't push the wrong button: lessons in life – or push two by accident.

What happens is that, first off, the user submits a query and sends it to his ISP, just like we saw in the skit. The recursive resolver sends it off to the authoritative name server to get an answer. The authoritative name server sends an answer back to the recursive resolver. Then that recursive resolver returns it back to you.

It's fairly straightforward. You need a question answered. Somebody else helps you with it, and they actually end up talking to a lot of people, as you saw in the skit. So in the end, Joe User goes to the right place. He goes to the web server that he wanted to get to.

At Parsons, we actually took the Firefox browser – I no longer work for Parsons, but when I did, we took the Firefox browser

and we actually modified it so that it would do DNSSEC validation on web pages.

This slide is an example of – you can see that big green DNSSEC checkmark. If you go to DNSSEC-Deployment.org today, if you're using a validating browser or a validating ISP – which, by the way, Google's public resolver does validation – you'll see the green checkmarks. If you don't have a validating environment that is not DNSSEC compliant, you will see the little warning sign that says, "DNSSEC is off."

Getting back to the hijacked example, to show how the "DNSSEC off" appears, we have an evil doctor now sitting on the bottom up there. Again, the user sends a query off to the recursive name server, but note that the evil doctor is right next to him.

So, he can respond really quickly, much faster than the ISP that has to go ask all these other questions, and say, "I don't care what you're going to ask for. I'm going to send you the same bad address for everywhere. I want everything to go through me."

What happens is that Joe User sends up getting redirected to an alternate website that the hacker actually can control. That's a little animation of the fact that the other information still happened and it got back to Joe User, but it came back so late that he actually didn't see the correct answer.

So DNSSEC is functionally equal to stopping this portion. It prevents anybody else from hijacking the information and assures that you're always getting to the right place – that Joe User will always get the correct answer.

These are not my slides, so I forget where the animations occur. I apologize for that. There's actually two other people that normally do this presentation tonight and you have the fill-in, I'm afraid. So, this is me. Fortunately, I know this information really well, too.

Going back to this example, that green checkmark occurred because DNSSEC validation happened. You won't get the DNSSEC-is-off logo.

Now, one other thing that I don't think most people realize is [that] if you go to something like CNN.com, do you have any idea how many DNS lookups actually occur to go to one webpage? It's a lot more than you would think about.

Actually, five or ten years ago, I worked with Russ Mundy at Parsons, and I told him to tell his laptop to use me as a DNS server, and I graphed every single query that went on just to go to CNN.com. Each one of those green and blue lines is a different DNS query for going to a single webpage. You can see that there's a ton of DNS traffic that you have no idea occurs behind the scenes – or the average person doesn't.

This is another pictorial example of, actually, the exact same thing laid out in a different way. It's pretty – all the little lines – but you can't imagine trying to understand that. Even experts wouldn't want to try to walk their way through looking up every image location and every JavaScript location and everything else that's needed to load a webpage.

That includes Facebook Like links. It includes Google Plus links. It includes "tweet this" buttons. All of those often end up in a different DNS request.

So, there are some basic DNS functions. There are some basic roles that exist in the world of people that work with DNS data. It's not just one person that actually puts all of this together. In the end, it's the data that matters, which is why DNSSEC is created to protect the data. So, no matter who else is involved, as long as that data is signed, again, it doesn't matter where it goes through.

This is an illustration of how complex even the data publishing mechanism is. We have up here on the left: I need to add this A-record to my zone, so I put it in the zone data. It gets published over into the authoritative server, which is where the recursive sever at the ISP asks questions to, based on the previously published data. The client, of course, is asking questions to the

recursive server. In a second, we'll see this diagram again with the DNSSEC bits added.

The DNSSEC implementation is mostly driven by these same functions with just some added information. DNS itself is made up of many parts, including the name server and the applications users and the zone publishers and the provisioning aspects.

Activities with large, complex DNSSEC functions are more likely to have complex DNSSEC implementation activities. Simply put, that says [that] if you have a really complex setup, DNSSEC will be more complex for you. If you have a very simple setup, it's actually quite easy to start using DNS.

As some examples, for a registry that's responsible for a large TLD operation, like .com, because they have to resign stuff all the time, it's a little bit more complex for them than the average person who only needs to resign rarely. They're not changing data very much. .com is adding new domains all the time, all day long.

A substantial enterprise with many components that are changing over time or changing on a regular basis, like HP.com on the slides, for example, probably have a lot more to think about to get DNSSEC up and running.

[For] Internet-based businesses with a number of business-critical zones, one important takeaway is that if you're going to do this on a business-critical zone, spend the extra time and energy to put it in a monitoring system to know when things go bad.

Unfortunately, we don't do that for DNS today. If somebody hijacks your zone, you probably don't know it because not many people actually put in the effort to monitor stuff as well. There are some companies out there with products that can help you if you just want to purchase and outsource that type of activity.

Then there's activities with not-critical DNS zones. Net-snmp.org is actually a software project that I host. It's slightly less critical. There's not as many people going to it. It's an open-source kind of project. It's not a bank. It's something that's still pretty important and it's actually a very popular software project.

And then, of course, [it's] your image's page with just your family sharing. There's different levels of protection there, so there's different levels of DNSSEC-type of infrastructure that can help you out as well.

Where does DNSSEC fit in all of this? It's required in order to prevent content from being spoofed. But an additional important takeaway is that it's only as good as you protect your own zone data. If you don't host your zone data on a decent

machine, then DNSSEC is not going to help you very much because the attackers would go off of your database that's easily hackable.

So, make sure that you protect your zone data just as much as you're going to protect it with DNSSEC. It does not fix your other issues with servers being hacked into and stuff like that. It protects the data on the wire.

Going back to this diagram, there's some additional new bits that we've added by throwing in DNSSEC. There is now a signing bit. After adding the data like we did before, instead of sending it straight to the authoritative server, we're going to sign it first and then publish the signed copy instead.

There's also this lock which represents the cryptographic keys that need to be passed between the signed data and the validating recursive resolver so that it knows that your data is valid.

As I mentioned once in the skit, the only real lock symbol that the validating recursive resolver needs is the root. Everything else it can figure out by asking com for the yourexample.com key, for example.

As a general principle, if you have a really active network, if you have a really active zone, then you should spend more energy

both in maintaining it as well as in protecting it with DNSSEC. DNSSEC scales in the same way that the DNS does. If you're doing very small trivial stuff, then you don't need much on the DNSSEC side. It'll still work. If you're doing a large, complex operation, you'll need a little bit more.

With that, we'll take a quick break for questions. There's some more slides in a little bit about how DNS – oh, actually that is the very last slide, isn't it? Excellent.

Matt Larson, you're in the audience somewhere? There you are. I'm going to give Matt an extra five minutes before we go onto the question part because Matt Larson from ICANN will talk about how the root keys KSK rollover is going to happen in the near future. Back to that diagram where that lock icon needs to happen. ISPs need to know about that transfer, so Matt is going to give us a quick overview about that.

MATT LARSON: Thanks, Wes. Hi, everyone. I'm Matt Larson. I'm the V.P. of Research in the office of the CTO at ICANN. I am one of the people who's involved in the project to roll over the root zone KSK. This is the key that we created in 2010 when we signed the root for the first time. That key hasn't changed in all that time. It's been the same.

We never intended for it to stay the same. In some of the documentation that we prepared, we said the key would be rolled after five years. It didn't say in exactly five years; it said after five years. And that's where we are now. I just want to talk a little bit about where we are in that project. We're in the middle of it right now.

The project is going to take a long time, actually, and that's on purpose. We want to do the change very slowly and deliberately. There's no rush for this. We're in normal operations. We don't have any reason to believe that there's anything wrong with the current KSK. So, there's nothing wrong with taking a slow, conservative pace on the project, which is what we're doing.

Here are some of the recent milestones. The new KSK was actually created last October. ICANN uses two different facilities where it stores the KSK – very secure facilities inside secure cryptographic hardware. The key was created in one facility and then moved to the other facility. It was created on the east coast and then moved to the west coast.

There's a quarterly cadence for using the KSK. Once a quarter, we bring the KSK out and it does its job of signing the ZSK. As a result, what we've decided to do is to fit all the events involved with the KSK roll into this quarterly cadence. That's why, in Q4 of last year, we created the new key. Then in Q1 of this year, we

moved it into the other facility – the west coast key management facility. Once that key was stored redundantly in two places, we called it Operationally Ready.

The next big milestone, which happened just recently, was at the Q2 key ceremony, where the key was actually published. It was used for the first time. As of now, the key is actually available and visible.

It's actually going to appear in DNS on July 11th – you see the date there – and the actual rollover itself is October 11th, 2017. So, I would be remiss if I didn't point out that that date is in bold on the slide. I should say it a few times: October 11th, 2017. That's the date you need to know when we stop using the current KSK and we start using the new KSK – what we're calling KSK 2010 and KSK 2017, respectively.

So by that time, if you operate any software that does DNSSEC validation that has the root zone KSK configured, you need to have changed it by then. So, that's why that date is so important. By October 11th, any DNSSEC validation software that has the KSK configured has to have the new KSK configured.

We have a whole bunch of information on this URL. There's a web page that's continuously changing and growing as we put more up-to-date information about the KSK roll there. If you

don't want to type the long URL, you can find it under the Quicklinks section.

I realize I had a very short presentation, Wes, because I wasn't expecting an extra five minutes. I also am going to be giving this material again, so if you're here and you come to the various DNSSEC meetings, you're going to see me and even more of this material at each of them.

Should I take some questions? Is that all right?

WES HARDAKER: Stay up here because this is our expert panel time. In fact, I'd like other experts to come up as well and join. There's microphones up here and anybody can answer questions.

The rest of the evening, we typically turn into a question and answer period. If you have questions about how to get started, what DNSSEC means, or how it works – Matt talked about key signing keys. There's actually two different keys used in DNSSEC. If you dive further into the complexity – we can always go deeper and deeper – but yes. I'll hand the answers off to anybody that wants to answer.

Please, won't you? First question.

MICHAEL OGHIA: Hi. My name is Michael Oghia. This is my first ICANN meeting and I'm a first-time Fellow.

WES HARDAKER: Welcome.

MICHAEL OGHIA: Thank you. I have quite a few questions about DNSSEC. I'll be honest: they might seem rather elementary to you, but I'm here, in part, because I want to learn more.

WES HARDAKER: You're in the right place. Please don't feel bad about any question you're going to ask.

MICHAEL OGHIA: Thanks. The first one is, how do DNSSEC and other security tools, like https, complement each other? Now, I recognize as well that https is at the application layer, whereas DNSSEC is at the protocol layer. I'm just curious as to how, together, this creates a kind of a suite of security for users.

I have another question as well, but you can either answer that now, or…

WES HARDAKER: Why don't you stay there and we'll let somebody answer that one. Does anybody want to take the answer for that one?

MICHAEL OGHIA: I can repeat it as well if you'd like.

WES HARDAKER: Jacques? Go for it. You're flipping. You get it.

JACQUES LATOUR: Okay, so DNSSEC at the DNS level makes the integrity of the DNS; To make sure, you go to the right web server. When you put in a domain name, DNSSEC will make sure that that happens; that the IP address you get is valid. So, DNSSEC doesn't encrypt that. It doesn't do any of what the https does. That's at the server level. So, that's your first part of the first question.

MICHAEL OGHIA: Sure. And just as a follow-up to that, why then would I need DNSSEC if I have https?

WES HARDAKER: Warren?

JACQUES LATOUR: Somebody else can…

WARREN KUMARI: There is some argument to be made that if you have https, DNS isn't quite as important because if you get to the wrong site, you'll probably detect that because they won't have the right certificate.

Unfortunately, that doesn't work in all cases. In some cases, you could get to a site that's run by an attacker who happens to have a certificate for you. That happened a while back in certain countries.

Also, if you don't have DNSSEC, an attacker could keep giving you the wrong answer and you would keep going off the wrong thing. That's more of a DOS instead of an actual issue where you give away your information.

DNSSEC also allows you to do a bunch of other [cool] things. You can build other things on top of DNSSEC. So, you can use that as an underlying protocol to build other sexy things on.

That was in no way a stupid question. [laughter] A lot of people really don't get the fact that they do different things.

MICHAEL OGHIA: Thank you. Actually, I understand now a little bit more what exactly is the difference. In terms of the data, let's say, that's being submitted over a website that's going through an encrypted https channel, whereas the initial site that I would be showed as an end user might be something malicious to begin with.

Thank you.

WES HARDAKER: Yeah, the Internet has layers of security. DNS can send you to the wrong place and there's no web security that's going to help you with that if you're at the wrong place. [laughter] Routing security is needed to get you to the right place, even if you know the address. Then application security is needed to actually make sure – so, yes, it's complex. Good question. Go on with your second one.

MICHAEL OGHIA: Thanks. I was just going to say that an attacker might have an encrypted website. Maybe they don't want to be spied on.

The second question now is a little bit different. Why don't all registrars offer DNSSEC for each and every – what's it called – TLD? Because, for instance, I have a .org address and my

registrar doesn't offer DNSSEC for it. I don't understand why. I'm willing to pay for it.

WARREN KUMARI: I don't understand why, either. You can always consider changing registrars. At this point, may registrars – probably most – do. Vote with your wallet. That's a perfectly acceptable option.

CRISTIAN HESSELMAN: Initially, they were not that familiar with the technology. Of course, for them it's an upgrade of their infrastructure, so they also need to see the benefits. You are actually one of the first people I hear asking for a DNSSEC-signed domain name because usually end users don't even know about the DNS. They just type in a domain name.

There's no real customer demand for registrars, so it's an infrastructure thing that the need to put in place. A37:nd there is not really a customer demand for it.

Many of the registries at least, and often also ccTLD registries, try to motivate their registrars to turn on DNSSEC signing, either through education or through an incentive program, which is usually a monetary program, to get these registrars to sign their domain names.

MICHAEL OGHIA: Thank you. I was actually just having a similar discussion a couple days ago at a different event. That was also on the lack of customer want for DNSSEC. I think I'm going to start writing e-mails to my registrars, saying, "Why don't you have it for .org? This is ridiculous."

WES HARDAKER: I definitely recommend that. There are, as somebody said, other ones that you can just a click a checkbox for and you're done. It takes care of everything for you if you use them to manage your data and stuff as well. So, it's a good thing.

MICHAEL OGHIA: Thank you.

WES HARDAKER: All right. I think we have one question online, and then there was another question over here – or two. Let's do the online one first.

JULIE HEDLUND: Thank you very much, Wes. The question is from Alexandrine Gauvin. She asks, "Does DNSSEC need to be enabled/activated at all levels (ISP, browser, TLD, registry services, hoster, software, etc.) to actually work?

WES HARDAKER: I'm looking for hands. Go for it.

ERWIN LANSING: The short answer is yes, at least for the DNS part. It needs have the whole hierarchy. From the root down to the zone you're looking at needs to be signed. And the recursor you're using has to look it up.

Not to get into too many details, but there are discussions about how close you need to get to the browser and how much you can trust the last mile from your ISP to your browser. If you want to be really secure, that means a secure channel as well. We're not there yet, but for at least getting it into your own network at your ISP, then you need the whole chain.

WES HARDAKER: Warren?

WARREN KUMARI: Yeah, I guess a follow-on from that. Most – in fact, I think all of the new gTLDs – are required to be able to support DNSSEC, and many other TLDs do as well. Many registrars do, but not all. A large number of recursive resolvers at this point do as well –

many of the big ones; for example, Google Public DNS and the Verisign one and many others also do DNSSEC validation.

Geoff Houston, who I don't think is in the audience, has some experiments that he has done that show that around 15% of all queries now are DNSSEC-protected. That does only protect you, though, as far as the resolver.

What would be really good is to have a secure way to get that answer to your machine. So, what's best is if your machine actually does its own validation instead or as well, and that's something which you can now do if you're willing to put in the time and effort.

DNSSEC-Trigger is a piece of software that will do it. There are also browsers which will do DNSSEC validation. Bloodhound is one, which is a Firefox clone or port.

WES HARDAKER: [Fork], yeah.

WARREN KUMARI: Yep. There are also extensions that you can add to your browser that will show you a little checkmark to show whether DNSSEC validation has been done.

WES HARDAKER: One of the important takeaways is that it is rollout process, so everything that rolls out early is protected early. So, it's not like you need the entire tree signed for everything to work. You need the pieces that you need to go look up to be signed in order for it to work. If you sign your zones and you register with a parent TLD that is signed, then your data is protected. If your competitor does not, well, that's their fault.

We have right now, I think, .5% of the .com zone – somebody can go look at SecSpider. We can actually get real, live numbers. But.05% of .com is signed. That seems like a small percentage, but it's like 5,000 domains under .com that are signed. That's actually pretty good. We're starting to see some real-world deployment.

WARREN KUMARI: And following on from that, there are also some TLDs which are requiring DNSSEC – .bank and .insurance, I think, both require that all of the domain names within that are DNSSEC-signed because they think that this adds useful security and helps users have more faith that they're getting to their correct bank.

WES HARDAKER: Okay. Thank you. I'm going to go to one question. There was somebody who had one over here.

CLEMENT GENTY: Hi. My name is Clement. I'm making a PhD and I'm a NextGen member. You told it – or if I remember – it was Jean-Jacques concerning the fact that DNSSEC is totally invisible for the final user. Is it possible that ICANN can ask registrars to offer DNSSEC for every domain? Why is it not an obligation to have the lowest scale of security through DNSSEC? Thank you.

WES HARDAKER: Matt? Sorry. There's a bus coming at you.

MATT LARSON: I want to make sure I understand the question because I didn't hear Jean-Jacques' earlier comment. Was the comment indeed about domains being signed or about the inability of applications to see DNSSEC validation status?

WES HARDAKER: If I understood it correctly, you're wondering why ICANN can't ask more of the registrars and the registries?

CLEMENT GENTY: If I wanted to make it a shorter question: why do we have to pay for DNSSEC? Why is it not built-in everywhere?

MATT LARSON: Boy, it is a bus headed at me, isn't it? [laughter] ICANN has been around longer than DNSSEC has had the deployment that it has today, so the legal agreements that govern the relationship and requirements of registries and registrars predate the widespread deployment of DNSSEC that we have now.

I think ICANN has done some things to promote DNSSEC. As Warren said, all the new gTLDs require DNSSEC. But I think there are certain aspects to, for example, registrar business models – if you look at the different kinds of registrars there are, there are all different approaches to being a registrar. The accreditation from ICANN to sell domain names is merely one aspect of different business models.

So, I think that's the area of something that just hasn't been specified by ICANN and that the market is handling at this point.

WES HARDAKER: Like many agreements that exist between governments and commercial entities or various bodies, there's a lot of preexisting stuff and they're not affected by new rules. I think, as you notice, any time new paperwork comes out – like on how all the new gTLD have to be DNSSEC-compliant – that's because they went through the new paperwork process.

There are companies under certain governments that are falling into the same category, where, as new things come online, you'll see more and more stuff saying they require it. More governments are requiring it internally, but there's a rollout process that involves replacing all this old stuff first.

We'll take a question to mic, and then I'll do you. Go ahead.

[SALVINALE SU]: Hello. I'm very new here – got a green label and everything that says "newcomer."

WES HARDAKER: Welcome.

[SALVINALE SU]: I'm also from the Norwegian chapter of the Internet Society. What I'd like to ask you guys is if you could give someone like myself some pointers on how we in the Internet Society or chapters can help you guys get some visibility to DNSSEC and, well, everybody. What should we do? Do you have some ideas, please? I'd love to hear.

MATT LARSON: Well, it's my job to mention the root KSK rollover at every opportunity, and you just gave me an opportunity. [laughter]

I would make sure that ISPs in Norway who have enabled DNSSEC validation and who have not heard the literally dozens of presentations that my colleagues and I have made know that by October 11th, 2017 – did I mention that date already? – they have to have the new KSK configured.

I know I'm making light of it, but in all seriousness, that's a valuable service. That's something we're trying to do with presentations like this, which is to get the word out that that's changing.

WES HARDAKER: Jacques?

JACQUES LATOUR: One of the good resources is ISOC. They have a Deploy360 program. If you go in there, there's a section on DNSSEC. It includes a lot of documentation. We actually spent a lot of time putting that together for beginners to understand the basics of the DNSSEC and all the way to implement it in ISPs, in TLDs, and in different regions.

Dan York, who's the prime person that works on that, actually spent a lot of time putting that together. So, that's for DNSSEC.

In the same place, there's a new thing: IPv6. It's old but it's new, and it's facing the same challenges that DNSSEC is facing: ICANN can't tell the world to do IPv6 and DNSSEC. They can recommend to use new protocols, but they cannot enforce. And that's the challenge that we're having now.

WES HARDAKER: Warren?

WARREN KUMARI: I just want to follow up on that. The Internet Society has actually been doing a great job of proselytizing DNSSEC. Dan York has done a bunch of stuff; .org as well, which is run by the Internet Society PIR. It was one of the first large signed TLDs, and is constantly pushing the envelope and improving.

What you can actually do is sign your zones and just talk to more people within the Internet Society in Norway and just suggest to them that it's a good thing. Explain to them what its benefits are, etc.

Seeing as Jacques mentioned v6, it's worth pointing out that there's something like 15% DNSSEC stuff. V6, with all of the work that's been going into it, is still substantially lower; depending on where you look, it's 1% or 2%. In some in some ways, yay, DNSSEC; and more work needed for v6.

WES HARDAKER: All right. Thank you.

[SUVINALE SU]: Thank you.

WES HARDAKER: Before we go on – I'll get to you in one second, and she's going to be first – what I failed to do is actually introduce myself and the panel, so why don't we quickly go through and say who we are?

I'm Wes Hardaker, by the way. I'm with the University of Southern California at ISI. Let's start at the end and work this way.

CRISTIAN HESSELMAN: I'm Cristian Hesselman. I'm with .nl, the registry for the Netherlands.

JACQUES LATOUR: I'm Jacques Latour. I'm with .ca for Canada.

ERWIN LANSING: Erwin Lansing for .dk for Denmark. Welcome.

WARREN KUMARI: Warren Kumari. I work for Google.

MATT LARSON: Matt Larson, ICANN.

WES HARDAKER: Go ahead, Julie. You deserve it.

JULIE HEDLUND: Definitely not an expert, but Julie Hedlund with ICANN staff.

WES HARDAKER: Kathy?

KATHY SCHNITT: Hi. I'm Kathy and I'm also with ICANN staff.

WES HARDAKER: All right. Thank you, everybody.

OLGA KYRYLIUK: I'm Olga. I'm a NextGen Fellow from the Ukraine. My question might sound very, very stupid, but just to clarify for myself, if the registrar doesn't enable this DNSSEC check, then I as an end

user has no chance to use this DNS check? And if I don't enable that on my browser also, then I will not see this green tick because, as you suggested, like 50% of the registrars are using this, but I've never seen this green tick. Does that mean that I just didn't enable that function on my browser or what?

WES HARDAKER: Let me start off by answering a little of that first. That green check is only on that one webpage. That was something that we did that would tell people to go to that webpage on THE DNSSEC-Deployment.org. I also may have confused you earlier because I tried to say that we had a browser that fixed that problem; but, if you were in a secured ISP that was using DNSSEC validation at its resolvers, you would see the green check, too. So, nothing on your part needs to be done if your ISP is doing validated resolving.

Anybody else want to add something? Matt?

MATT LARSON: I think it's important to distinguish; pretty much any time you talk about DNSSEC, it helps to keep in mind that there are really two major parts of it. There's the signing side. If you have DNS data that you're responsible for; if you have a domain and it's

live on the Internet, you need to participate in DNSSEC. You need to sign that data. So, that's the signing side.

On the other side: for anybody who looks up that data – that's the validation – if they're using an ISP or if their enterprise has enabled DNSSEC validation, then they can consume the signed data in your zone and validate it.

Both of those things have to be working for you to get the benefit of DNSSEC. If you sign the data and make your signed data available but no on looks it up and does validation, then that's only half of the piece. Likewise, if you're doing validation but on the mini-domains that aren't signed, there's nothing to validate.

When you talk about this in a registrar context, we're probably talking about the ability as the owner of a domain to put in the necessary DNSSEC information so that your domain is plugged into the rest of the DNS hierarchy.

That's on the signing side, but there's still a whole validation side that registrars are not typically involved in. That's typically ISPs and large enterprises.

CRISTIAN HESSELMAN: I was going to say what Matt just said.

WES HARDAKER: All right. We had another question.

WARREN KUMARI: And I believe you said Ukraine. I quickly checked the Ukraine's ccTLD. It's signed, so that's at least part of the way there.

WES HARDAKER: Thank you, Warren.

CLAIRE CRAIG: Hello. Good afternoon. I am from Trinidad and Tobago. I am an IXP researcher, but I am asking this question from my other hat as a CaribNOGer. I am a member of CaribNOG.

When these things come up, I am always concerned from the end user's perspective because we are doing so much to get the unconnected connected. But a lot of the times, the end user gets connected and they do foolish things on the Internet because they really don't know.

So as an end user, I don't want to know about DNSSEC or I may not know anything about DNSSEC. How do I stay safe on the Internet? How do I get information to lobby my IXP or my government or whatever? What do I need to know as an end user to be safe on the Internet?

Because part of what we do is teach people how to be safe on social media. Similarly, should we be having these kinds of initiatives for end users? Thank you.

WARREN KUMARI: I'm sure there'll be many other answers to this as well. You as an end user, assuming that your ISP has DNSSEC enabled for you, shouldn't need to do anything, shouldn't need to know anything. If there is a DNSSEC problem, you just won't be able to get to that website. If there has been an attack which poisons the DNS, you just won't be able to reach that and it will look as though it has failed.

If you want to be able to get there, lobby your ISP to please enable DNSSEC validation on their resolver. Or, if you use one of the large resolver, that might already do it for you.

I should point out that that doesn't keep you safe online. That's just one part of it. You still need to make sure that you're not posting stupid stuff on social media or clicking on random links, etc. This is just one small part of it.

CLAIRE CRAIG: Yeah, but the point is that I may not know anything about DNSSEC, so I can't lobby my IXP. There are ISPs who say, "We can't afford it." As the person said before, they may have to

change out their infrastructure. Therefore, they're not interested in doing this right now.

What should users do to ensure that the Internet is safe?

MATT LARSON: Warren can't say this because he works for Google, but users could switch to a recursive name server that does support DNSSEC. The largest of those is the Google Public DNS, but there are others, as Warren said earlier. Verisign runs one. I'm sure there are others. I just don't know them off the top of my head. So, that's the biggest thing that users can do.

Again, that requires some level of sophistication as a user: to go into your configuration and change away from the defaults. Certainly, if an ISP is willing to enable validation, that's the easiest way to go to get DNSSEC protection for its users.

But users do have the ability to vote with their feet, as it were, and move away from the ISP's recursive name servers that they're configured with and switch to others.

WES HARDAKER: Almost every operating system out there lets you override the DNS settings and say, "I want to use the different resolver." But it's in the advanced section of most settings.

WARREN KUMARI: A very short thing from Matt's thing. I've looked at Geoff Houston's site – he collects a bunch of statistics on this – and around 3.3% of people in Trinidad and Tobago currently do DNSSEC validation already. So, at least it is supported by some set of the ISPs.

WES HARDAKER: All right. Somebody had a hand up. Was it you that had a hand up? Okay. Yeah, go ahead and come up.

Okay. And then there was one more over here, too. Thank you.

SIMON SOHEL BAROI: My name is Simon. I came from Bangladesh. I have a very dumb question. This year America got a new president, President Trump. Very good. Last year we got the IANA transition. Very good. But you said that you keep those 14 keys in two different locations inside the U.S.A. Why not do different sides of the world? That's one question.

The second question is another dumb question. I came from a very LDC (Least-Developed Country). That's what the U.N. said, I should say. In these countries, we saw these kinds of projects – like DNSSEC, IPv6, and RPKI. All these kinds of projects don't go

very well. DNSSEC started like ten years back. RPKI started like five years back. IPv6? Before I touch my laptop.

Why do these kinds of projects not see the light? You said that Geoff Houston said like 17% of the world – and now he's having DNSSEC resolvement. Why?

Two questions.

MATT LARSON: All right. I guess I'm the person to answer the first question. When we signed the root in 2010, that's when ICANN still had the relationship with the U.S. Department of Commerce. Part of the requirement for signing the root was that the root KSK material be within the United States. We of course wanted redundant facilities, so we ended up with east coast and west coast as just about as far about as we could do, given the requirements.

You raised a point that many other people have raised, both in the lead-up to the IANA transition and now afterwards, which is, "Well, what about one outside the United States?" I think that's a very reasonable question. I think that would give us all kinds of extra opportunities. The more of these facilities we have, the more you can avoid fate sharing, if you will, between keys.

All that being said, that would be a significant move for ICANN to undertake; and it would certainly be a very, very expensive move

to provision one of these new key management facilities. Certainly, it would be very complicated because I imagine there are multiple countries that would be interested in hosting all that.

All that being said, that's something that ICANN the organization, I think, really needs to get the lead from ICANN the community. I think, if that's something about which the community keeps saying loud and clear that this is a priority, that "We think there should be additional key management facilities outside the U.S.," then that's input to the policy process. That's something that then can be prioritized with all the other things the community asks ICANN to do and spend resources on.

JACQUES LATOUR: I'll answer the second part.

WARREN KUMARI: Actually, can I quickly carry on with the first part a little bit more?

Yes, the keys are both in the U.S. However, in order to actually use the keys, it requires a bunch of trusted community representatives to come along, and the trusted community representatives are drawn from a bunch of different countries.

So, whenever the keys are actually used, people fly from other countries to actually come along and show up and do stuff.

The keys are in the U.S., but they're locked in secure enclaves. If anybody tries to open them, all sorts of alarms go off and bad things happen. So, yeah, that is definitely a scary thing, but it's slightly less scary than it sounds at first blush.

JACQUES LATOUR: Your second part is: how come it's taking so long? IPv4 has been operational for about 45 years. I think it's about time that we started thinking about retiring it. DNSSEC has been there for a long time. The main reason it's hard to do anything is because humans, I guess, resist change. They like the old ways. For some reason, we love IPv4, and we're trying to find ways to make it last even longer.

So, I'm a big proponent of shutting down IPv4 and moving to v6. When I talk about that with some people, they go, "You want to do what? Shut down v4? You can't do that."

So, it's change. Managing change on a global basis is very difficult. That's what we're facing.

CRISTIAN HESSELMAN: I think, in addition, the change would happen quicker if there would be a customer demand, for example. That's not there in this case. It's really an infrastructure update that we need to realize as a community.

Also – I wanted to make a second point but I forgot that one.

WES HARDAKER: A lot of new technology of any type has a cost associated with it. ISPs and everybody has to weigh all the things they want to do and what the costs associated with it is. Unfortunately, sometimes security gets pushed lower in the sack because it doesn't have any immediately visible component until somebody gets attacked. That's the common problem. So, with the RPKI and DNSSEC and IPv6, there's a huge cost for doing each of those. So, it takes time.

JAD EL CHAM: Hello. I'm a first-time ICANN Fellow. I come from a purely technical background, so I have a purely technical question. We have seen recently over the last couple of years more and more vendors providing security over DNS in terms of relaying DNS queries to DNS providers on the Cloud. Typically, they would have scrubbing centers. They would identify the DNS query and get back to us with an answer.

One of the solutions is, for example, OpenVPN, which was acquired by Cisco. I've also seen antivirus or antimalware software that, when we install them on our PCs, ask for permission to reroute and change the DNS servers that any PC would use.

So, my question is two-fold. These kinds of solutions – are these an alternative to DNSSEC? Because if you take a look, for example, at the OpenVPN, they alone handle like 2% of the whole DNS traffic – queries, at least. The second question: do they go along?

IRWIN LANSING: I would say they go along in the sense that those trusted services do some kind of vetting of the answer for you. DNSSEC would be part of that vetting they use to make sure to give you the right answer. They also use other stuff like known blacklists of viruses or malware sites. But DNSSEC definitely is part of what they should use before they give you an answer.

WES HARDAKER: Okay. Anybody else? All right. Thank you. I am jumping around properly in queue management, but it's not as easy as you think.

RACHEL POLLACK: No problem at all. I was sitting there, so I came to the microphone to ask it.

WES HARDAKER: I appreciate that. Thank you.

RACHEL POLLACK: My name is Rachel Pollack. I'm here as a NextGen Ambassador and I work at UNESCO on Freedom of Expression. I'm also from a non-technical background. As a preface, today is the World Day Against Cyber Censorship by Reporters without Borders. My understanding is that one form of Internet censorship can be in the form of DNS redirection.

I wondered if DNSSEC can play any role in getting users to the correct sites. If that is the case, have there been any kind of political or other kinds of resistance to DNSSEC on those grounds? Thank you.

WARREN KUMARI: I have two answers here. Yes, DNSSEC can at least help prevent censorship through the DNS or at least make it clearer that it's happening. It might not be able to actually stop the censorship, but at least you can tell that somebody is fiddling with the DNS queries, which at least helps expose it.

As you say, a lot of censorship is done with the DNS. Lots of ISPs or countries will watch for specific queries and stop them. This is something that the IETF is taking very seriously. I actually chair a working group called Deprive.

We're trying to deprive the attackers of the DNS information. What that does is it encrypts the DNS query from your client machine to the recursive resolver. That way, censors can't actually see that you're trying to reach a site that they don't want you to go to, so they can't then block it.

This is starting to be deployed and should go a long way towards dealing with censorship and privacy issues.

MATT LARSON: I guess I'll make a comment that, in most cases, if someone is going to do censorship or otherwise change DNS answers, the same place that happens is where DNSSEC validation often happens, which is in the recursive name server at an ISP.

The issue is – I will dramatically hold up my phone – my phone is configured to use a recursive name server somewhere. That's typically where the validation happens or where the content filtering would happen. Now, we designed the DNSSEC protocol so that my phone could do DNSSEC validation itself and not

trust the upstream, if you will – one of my fellow panelists referred to "the last mile."

That's what we call the last mile issue, which is that, right now, you pretty much have to trust what your recursive name server is telling you. If they're doing DNSSEC validation, all the better.

Because of various reasons like how old some of the software is and APIs are and institutional inertia and many other reasons, DNSSEC validation hasn't made it to end user devices yet in any scale whatsoever. But that would be the way that, as Warren said, you would at least be able to detect that somebody was tampering with the results that you were seeing.

WES HARDAKER: I think that that is probably where we'll end up in the long future. He talked about a phone. I actually ported our DNSSEC stack to an N900, which hasn't been produced in five years. I think all of our working examples died because the phones no longer work anymore.

So, it's very much possible. DNSSEC is not so special that it has to be in great, big things. Actually, small devices can implement it easily as well.

Okay. Did you have any…

RACHEL POLLACK: Excellent. Thank you.

WES HARDAKER: Thank you very much. I think – yeah, go ahead.

[SHOA ABODI]: I work for National Internet Exchange of India. I'm also working under an IGF project – the Indian Internet Governance Forum in India.

One of my roles in my job is to advise the government of India on the proposals submitted by the technical society. Recently, one of the technical societies submitted a proposal to set up a DNS Center of Excellence in India. They asked a few questions to us, like, "Why should we set up that kind of center in India, and what is the use?" I started a report, published by ISOC. They assured the deployment of DNSSEC and they assured us that that is related to that.

I advised them that way. I divided the whole process into two phases: set up a DNS Center of Excellence in India and conduct a study in the area where we have the facts/knowledge on the subject limited amongst the ISPs, registries, registrars, and website owners.

They are also facing our challenging by implementing and upgrading their network and implementing DNSSEC.

In the second phase, after the successful completion of the first phase, we may start training in certification programs for ISPs and make it mandatory for the government websites, like NIC, the [inaudible].gov in India, to implement DNSSEC and also make it mandatory to implement DNSSEC on the websites which are already being registered and used, as well as in the new applications.

I would like to know how ICANN can play a role in this and the technical support the technical society can get from ICANN.

WES HARDAKER: Jacques, did you want to go first while he's thinking?

JACQUES LATOUR: So, you're talking about implementing a DNSSEC Center of Excellence, right?

[SHOA ABODI]: Yes, developing a kind of center where we can –

JACQUES LATOUR: The answer is: yes, do that. Because there's a lot of innovation done around DNSSEC that goes beyond just the DNS queries themselves. If you go to the workshop on Wednesday, you're going to see a lot of new technology being developed on top of DNSSEC that enables e-mail encryption and that enables SSL verification. It's called DANE. So there are new protocols being built on DNSSEC that can change the Internet.

So for sure, you can do that. I think ICANN has resources to help on the training for that.

[SHOA ABODI]: Another guy also mentioned the same issue with ICANN. We conducted a workshop in Mumbai also. We invited a lot of ISPs there for the workshop, but still people are not implementing DNSSEC. They come to the training and they're not implementing. That is the issue.

So, we are planning first to make it mandatory for the governmental websites we are having. We will show an example, but before that, we want technical support and technical learning from ICANN. So, whom do we contact for that? I would like to know so that we can jointly develop some kind of a DNSSEC Center of Excellence in my country.

MATT LARSON: I do support that. I think that's a great idea. Some of my colleagues in the office of the CTO at ICANN do DNSSEC advocacy and DNSSEC training. We, like any organization, are stretched thin for bandwidth, so I don't know how much we could help in terms of actual personnel training.

I could put you in contact with my colleague, Rick Lamb. He's not here to defend himself, so I'll give you his name. But in all seriousness, Rick has been a tireless advocate for DNSSEC deployment and has done DNSSEC training all over the world. That's one of the things he does. So, that's the first thing that I think of when I hear your request for help from ICANN.

I guess I would also say to come to ICANN meetings because this is the place; rooms like this – Julie will probably be happy if I pitch the DNSSEC workshop on Wednesday that you see on the screens behind me. That's a place to meet colleagues who are also working on DNSSEC and also active in the industry.

So maybe that's not help from ICANN the organization, per se, but it's at least helping facilitate connections with other people who are doing the same sort of thing.

WES HARDAKER: Okay.

WARREN KUMARI: I guess I'll just follow on from that. When you say that people aren't really implementing, it turns out that India actually has a somewhat higher than average DNSSEC validation.

[SHOA ABODI]: Yeah. That is because India has a very huge user base. We have around 400 million Internet users. So, you compare the statistics with that number, it's still really small and the risk is big.

WARREN KUMARI: Even percentagewise, India has around 17% of people validating, which is a little bit higher than the global average. But at least there is some progress.

As for possibly getting government sites DNSSEC-signed, one of the big things which got a fair bit of initial movement for DNSSEC is that the U.S. government initially said that all .gov domains have to be signed.

That made a huge amount of progress at actually getting DNSSEC done, and also a fair amount of progress towards people just teaming up and fixing their DNS infrastructure. Things are now somewhat better in the [inaudible] zone than they used to be.

WES HARDAKER: That effort of the U.S. government actually helped create a lot of the tools that are now in use by a lot of other people because they were one of the earlier adopters.

Okay. There was another question in the back.

ABDERRAHMAN AIT ALI: Hi. My name is Abderrahman, a NextGen Fellow. I have a very quick question. It's actually about the transition costs. I'm curious about how easy or how hard it is to transition from DNS to DNSSEC. Are there enough incentives for those who are responsible for doing the transition to do that exactly? That's it.

CRISTIAN HESSELMAN: For at least registrars within the Netherlands, we had this incentive program where we would give them a discount on the domain names that they would register with us. I think there are similar programs in Sweden and other registries just to lower the threshold a little bit, in financial terms, for them to start signing domain names.

Then there's the other side of the coin, which is with the ISPs. For them, at least from where I come from, it's not so much the cost that they're afraid of – at least not the cost of implementing DNSSEC validation – but the potential support calls they're afraid of getting, because of validation errors, for example.

That's something they're afraid of, but at least large ISPs in the Netherlands have now decided to move to DNSSEC anyway.

It's also a lack of understanding of the technology in this case. So for those organizations, it's not so much the costs of the technology but the stuff that's around it. For the registrars, which are, at least in the Netherlands, usually smaller companies, it's the cost of the implementation of the system. So, it's two different types of costs, if you know what I mean.

ABDERRAHMAN AIT ALI: Yeah, but everything can be reduced to a cost or money, right? Time is money and capacity-building is like taking –

CRISTIAN HESSELMAN: Yeah. For the registrars, we used an incentive program because we have a customer relationship with them. The ISPs are basically deciding on their own whether or not to start validating.

Did that answer your question?

ABDERRAHMAN AIT ALI: Yes. Thank you very much.

WES HARDAKER: All right. Thank you very much. We have time for another question or two, maybe. Go ahead and come up. Yes, thank you.

CHAWANA HUANGSUNTORNCHAI: Just a quick question. My name is Chawana. I'm with NextGen's program. Is there any possibility or has it happened that it has been verified by DNSSEC, like, "Okay. We can see the green tick box on the URL box," but it's still a fake one?

WARREN KUMARI: So…

WES HARDAKER: You spoke first.

[laughter]

WARREN KUMARI: So, as far as I know, there have not been any technical DNSSEC issue/problems. So, there haven't been any cases where DNSSEC has incorrectly shown the checkbox.

However, you have to keep in mind what the checkbox means. All it means is that the data that came out of the DNS is the information that was put into the DNS. So if somebody types in

the wrong DNS address when they're configuring their DNS server, DNSSEC will still show you the checkmark, even though what the person typed in was incorrect. So it just validates that the correct information came out that was put in by the person who owns the zone.

CHAWANA HUANGSUNTORNCHAI: So that means if junk is put in, it is the junk coming out.

WARREN KUMARI: Garbage in, garbage out.

CHAWANA HUANGSUNTORNCHAI: Okay. Thank you.

WARREN KUMARI: But there have not been any cases of DNSSEC incorrectly saying something was valid when it wasn't. So no technical problems with it.

CHAWANA HUANGSUNTORNCHAI: Thank you.

WES HARDAKER: I've spoken to a lot of the browser authors, and they are really trying to clean up their interface. They've never been entirely certain that the green and red in a URL bar helps even on the https side. So, there's a lot of debate on what's the proper way to show that to a user and when. I don't think that the answer is entirely there yet.

Julie, you have a remote question, please.

JULIE HEDLUND: Thank you. We have a question in the chat room from Alexandrine Gauvin. The question is, "How can I check if an ISP is DNSSEC-signed?"

WES HARDAKER: That's a great question, and I wish that we had a list. Warren?

WARREN KUMARI: I believe that you still a DNSSEC and valid name, so you could try to go to the phishing page thing and see if you get the unhappy or not. That's at least how you can do DNSSEC validation to see if it's signed DNS [inaudible] maybe.

WES HARDAKER: Right. There's a few domains that you can go to that will tell you if you are behind an ISP that's doing validation. The sad thing is I

created one or run one and I'm blanking on the name of it. It's like DNSSEC-ready, I think.

Can you look that up? Find it.

But DNSSEC-Deployment.org has the one with the checkbox at the top. The other one that I was referring to that we'll get for you in a minute has a big thumbs-up or thumbs-down. It's incredibly obvious. It fills the whole page.

CRISTIAN HESSELMAN: I have a .nl-specific answer. We have a website where we show the percentage of traffic that we receive that's asking for DNSSEC key material. That suggests at least that the origin of the traffic is DNSSEC-enabled, so it's validating signatures. We actually put names of ISPs with that. So if you look at our site, you can see which ISPs are actually asking for signatures in the DNS.

WES HARDAKER: Actually, in the Android marketplace, I create a tool many year ago that actually does extensive tests of your ISP's resolver, and not just whether it does DNSSEC and checks validation. It's how compliant it is. It gives you a bunch of green and red dots accordingly. But it's really meant for experts to go look. But if you see a whole bunch of green stuff, you know it's good.

Anybody find the other website? I need to go look in my…

UNIDENTIFIED FEMALE: [inaudible]

WES HARDAKER: Yeah, there's a few. All right. We probably have time for one last question. Does anybody have one last question? Yeah?

UNIDENTIFIED MALE: Hello. I would like to ask you a little bit about a kind of system level question about DNSSEC and how DNSSEC interacts with the Internet or Internet security.

If this problem of DNS and security is solved, is there some sort of theory or do you have a hypothesis about where security problems will move to from the DNS? So, if I'm attacking DNS, you fix DNS, where do I attack next?

WES HARDAKER: Good question. Anybody?

CRISTIAN HESSELMAN: That would probably be the IOT.

UNIDENTIFIED MALE: Yeah.

[laughter]

CRISTIAN HESSELMAN: With all kinds of leaky devices that can easily be hacked into. I think that's also a major challenge if you look at the security issues on the Internet right now.

WES HARDAKER: And you hit on a very fundamental point, which is that the Internet started off very small and not secure and we've had to piecemeal these solutions on top of it. So, there always does seems like there's a next one.

Matt, did you have something to add? No? Okay.

All right. With that, I would like to thank our panel for helping us out with answers today. If you could give them a round of applause, I'd appreciate it.

[applause]

I would like to point out that there's some other research that you can get this week. You'll hear DNSSEC actually talked about in a number of places. You'll hear some presentations on Tech

Day, which is on Monday, as well. There's a whole set of technical stuff. If you're into the technical market for information, it'll saturate you with more information than you can handle. There's almost always some DNSSEC presentations in that.

On Wednesday, we have an entire day devoted to DNSSEC, from 9:00 until 3:00 in the afternoon. There'll be an all-day workshop. It is fantastically held. It's actually what got me to my first ICANN meeting a long time ago. I'll be there for at least half of it.

In fact, I'll be running the DNSSEC Quiz. Some of the information you saw on the slides today will be on the quiz. So, just by coming here, you could have a right answer for the quiz, even though you knew nothing about it before today, if you were really paying attention to the bullets.

Julie?

JULIE HEDLUND: Well, I wanted to say thank you for that plug there, Wes. Please do come. It's a very fun workshop.

I'd also like to ask you all to join me in thanking Wes for doing a great job and stepping in yet again when we needed him here. Thanks so much.

[applause]

WES HARDAKER: Thank you. You didn't give me a chance to thank you first. Julie and Kathy put this on every single time, and they manage to get the T-shirts here and manage to get the right people to fill the T-shirts. The effort does not go unnoticed, so thank you to both of you for putting it on year after year.

All right. Thank you all for coming, and I hope you enjoy your evening.

[END OF TRANSCRIPTION]