KOBE – DNSSEC for Everybody: A Beginner's Guide
Sunday, March 10, 2019 – 15:15 to 16:45 JST
ICANN64 | Kobe, Japan

WES HARDAKER: We will fix that in one second. It's going to be in all of them now too. Good.

Alright. So, today we're going to talk about what DNSSEC is and how it protects your Internet usage and everybody's Internet usage, and how ICANN is involved in it. I'm Wes Hardaker, I'm from USC Information Sciences Institute. We have a cast of wonderful characters behind us that will join us in a minute, and I will introduce them in a minute.

In the meantime, I'd like to tell you a story about DNSSEC, how it actually began. Well it began a long, long, long time ago in 5000BC back in the age of dinosaurs. And, it started with Ogwina – this is our main character for the day. She lives in a cave on the edge of the Grand Canyon. This is Og. He lives on the other side of the Grand Canyon, also in a cave. They're really far apart. The Grand Canyon is very deep and very wide. It's a long way down, and they don't get a chance to talk very much – they're so far away.

On one of their rare visits, they crossed the channel and they're talking to each other, and they noticed that there's smoke coming from Og's fire and they think this is a possibility. We can

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

communicate using smoke signals. And pretty soon they're chatting regularly, and they're chatting back and forth using smoke, and all is going well. Until one day mischievous caveman, Kaminsky, moves in next door and starts sending smoke signals at the same time.

Now Ogwina is really confused. There are two sets of smoke signals coming from across the canyon and she doesn't know which one is which. So Ogwina sets off down the canyon and tries to sort out the whole mess. Ogwina and Og consult the wise village elders. Caveman, Diffie – now some people apparently know who Diffie is. Diffieis a famous Cryptographer that helped develop the technology behind DNSSEC and we'll go into that. But he runs into the back of Og's cave, where he finds some magical blue powder. And, it's strangely colored, and he runs out to the fire and he throws it on the fire, and because the magical blue fire turns into blue smoke, now Ogwina and Og can continue chatting happily because only she has to believe the blue smoke, because the blue dust only exists in the back of Og's cave.

So, everybody was done, right. We're done. That was the introduction to DNSSEC – you understand it perfectly. So, we're going to explain it in greater detail but the concepts behind that, the concept behind a magical thing that sort of turns one thing into something that you know it came from the right place, is exactly what happens in DNSSEC.

So, let me dive back to DNS a little bit, and we'll begin at a high-level concept of DNS itself. If you've looked at DNS or you've gone to the DNS for Beginners Tutorial earlier in the day and earlier yesterday, they probably showed you a diagram like this – the DNS starts at the very top, it starts at the root, which is heavily discussed at ICANN, and then underneath that are all the TLDs, and sometimes there are country codes, sometimes there are things like com, and then underneath that are second-level domains like co.uk and bigbank.com and nic.ma. Today, we're going to concentrate on bigbank.com.

So, the important thing to know is that your ISP has a resolver, and the resolver knows where the root zone is, and as long as it knows where the root zone is, it can follow this chain downward to figure out where everything else is. So, it has to start at the root, and then it goes down and it knows, okay, where's com, and then it goes down and we'll go into greater depth about that with an example here in a minute, but basically, each level refers the resolver to the next level down. So, the only thing it has to know at the beginning is just where the root is. Eventually the question is answered and then the resolver actually caches that information for a while for future use.

Here's the problem. There's no security in DNS. When it was invented, I don't know what year, a long time ago – 84, there was no security added to it. Everybody was just good back then, there was no evil, and the names were easily spoofed later on, and people realized that they could work their way around the system and give you a bad answer, and caches are easily poisoned, so the resolver might remember not just a good answer for a long time, but it'll remember a bad answer for a long time as well.

So, to further illustrate this I'd like to bring forth the cast of characters that I have up here in these white shirts, and so, they're going to walk you through an example of exactly what your resolver does and what an ISP does, and we'll start off with Joe User here on the left. He's going to have to do some banking today at bigbank.com, so, he'll start off doing some banking and we'll see how the DNS leads him to hopefully the right answer.

UNIDENTIFIED MALE: They want you to see me.

RUSS MUNDY: Hey, ISP.

WES HARDAKER: Yep.

RUSS MUNDY: I need to talk to bigbank.com. Here's the name of the guy.

WES HARDAKER: I don’t know where bigbank.com is. Let me go try find that out for you; I’ll be right back.

Hello root, I would like to reach www.bigbank.com. Can you please tell me where that is?

UNIDENTIFIED MALE: Hi, I’m the Root Zone Server, I know about the top-level domains, so, you’re looking for .com? Why don’t you go to the dot-com server at 1.1.1?

WES HARDAKER: Okay, sure, let me go to that. Hello, dot-com. I’m looking for www.bigbank.com. Could you please tell me where I can find them?

UNIDENTIFIED MALE: I don’t know where www is but I can tell you where bigbank.com is. He’s at 2.2.2.2.

WES HARDAKER: Hello there, I’m trying to reach www.bigbank.com. Can you please tell me where I can find that?

RUSS MUNDY: Yes, I can, I am bigbank.com and I know where www.bigbank.com is. It is at 2.2.2.3.

WES HARDAKER: Awesome. Let me go tell my user.

RUSS MUNDY: And, he might want some of his money.

WES HARDAKER: Hello, apparently you connect to 2.2.2.3. That's where www.bigbank.com is.

UNIDENTIFIED MALE: Thanks bigbank.com.

WES HARDAKER: Yeah. Alright. Thank you, silly players of the DNSSEC Tutorial. We appreciate it. We'll come back to you in a second. Yes, please give them a round of applause. But wait, it's going to get better. Alright, next slide please.

So, that whole skit was very similar to how Ogwina was chatting with Og, through the resolver, and getting the signal before the evil came about. So, the question is what happens with the evil Kaminsky that came forward and produced an alternate smoke signal? So, how does that affect DNS? How can DNS be spoofed? And how can problems arrive?

So, we're going to go through the exact same skit again – it'll be exactly the same – I promise.

RUSS MUNDY: Hello, ISP.

WES HARDAKER: Hi.

RUSS MUNDY: I need to make a deposit with bigbank.com. Could you please go find this guy?

WES HARDAKER: Sure, no worries. www.bigbank.com. I'll go along and ask the root.

Hello root, one of my users would like to reach www.bigbank.com. Can you please tell me where he is?

UNIDENTIFIED MALE: I can tell you to ask the dot-com server at 1.1.1.1.

WES HARDAKER: Good enough, I guess I'll go and ask him. Hello dot-com servers. One of my users wants to reach www.bigbank.com . Where is that please?

UNIDENTIFIED MALE: I can't tell you www is but I can tell you bigbank.com is at 2.2.2.2.

WES HARDAKER: Cool. I'll go along and ask there. Hello, one of my users wants to reach www.bigbank.com. Can you please tell me where that is?

UNIDENTIFIED MALE: Sure. No problem.

WES HARDAKER: Cool.

UNIDENTIFIED MALE: www.bigbank.com is at 6.6.6.6.

WES HARDAKER: Sure, thank you. Hello user, you should go to 6.6.6.6. That's where www.bigbank.com is.

RUSS MUNDY: Sounds good. Or whatever. So now I was going to—

UNIDENTIFIED MALE: I'll take that deposit sir. Thank you very much.

WES HARDAKER: Alright. So, you can see the problem, right? Poor Joe User really doesn't know what answer to believe. He believes the first one that he gets. And so, this is the issue with the smoke signals, just like before, where there's actually two signals and the user tends to believe one of them, and they sort of have to pick randomly, and in this case, Ogwina really doesn't know which set of smoke signals to believe.

So, back to our high-level concept of DNS. We talked a bit earlier about the roots at the top and coms underneath it, and then bigbank.com, and if your resolver at your ISP is talking to the wrong system, it might get a good answer, the blue one, or it might get a bad answer, the red one.

So, DNSSEC fixes this, and this is why you're here today. DNSSEC adds back in security to the DNS where it didn't exist before, and it does this using digital signatures. It does two important things. It says that the information has not been tampered with at any point along any of the transfers, and it says that it originated from the right place. You can guarantee that it came from the right original location, even if it was stored on the bottom of a shoe or something like that. It was signed and it was valid forever. The keys in signatures are stored in the DNS itself which makes it really nice, because in order to figure out whether it's secure or not you can actually use the DNS itself to do those look-ups and figure out what keys you need, and we'll see an example of that in a second.

A resolver only has to … Just like a resolver before only had to know where the root servers are to start with them and then they can chain all the way down, DNSSEC is the same way. The resolver has to know where the root servers are and they have to know that one root key, and then they can build a chain of trust below that, as each level signs the key of the next level until the chain is complete. So, as long as you follow that cryptographic chain all the way down, you know that you're getting the right answers.

So, now the advantage is, back before when we had this diagram, Joe User didn't know which one to believe. He didn't know whether to believe the blue or the red. Now we can actually validate and show that the red one won't match. It won't work.

So, let's fix this in our play and we'll see if – can you guys do it with more good, less evil?

UNIDENTIFIED MALE: That was awesome.

RUSS MUNDY: Hey, ISP, I need to talk to bigbank.com, and I need to know that it's a valid answer.

WES HARDAKER: Okay, fair enough. Let me go figure that out for you. Hello root, one of my users wants to talk to www.bigbank.com. Can you please tell me where that is?

UNIDENTIFIED MALE: I can tell you where dot-com is, it's at 1.1.1.1 and here's the certification that shows that that information is correct.

WES HARDAKER: Okay, great, I will trust that. Let me go along and ask the dot-com servers.

Hello there, guess what? One of my users wants to talk to www.bigbank.com. Can you please tell me where that is? And I'm going to check your signature when you do.

UNIDENTIFIED MALE: Sure, you seem to ask for that a lot. I can't tell you where www.bigbank.com is but I can tell you where bigbank is, it's at 2.2.2.2 and here's the signature.

WES HARDAKER: Great. I will go along and ask. Hello there, I would like to know he address for www.bigbank.com. Can you please tell me?

UNIDENTIFIED MALE: Bigbank.com is at 6.6.6.6.

WES HARDAKER: Okay, hang on a minute. Where's the signature?

UNIDENTIFIED MALE: I don't have that. Oh, no!

WES HARDAKER: I'll ask someone else – I don't trust you, scummy dude.

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

RUSS MUNDY: Well, I do know www.bigbank.com is at 2.2.3 and here is the signature.

WES HARDAKER: That looks valid. Hello Mr. User, bigbank.com is at 2.2.2.3 and I checked the signature and you can rely on that.

RUSS MUNDY: And I see the signature here, and I thank you for that. So, thank you Big Bank. Send money.

WES HARDAKER: Alright, thanks very much. Can you give our performers a round of applause please? They do a great job. If you're at future ICANN meetings we do this every time. Anybody seen this skit before? A couple of people, yeah.

UNIDENTIFIED MALE: [inaudible]

WES HARDAKER: So, this is equivalent to the blue smoke. Right. Ogwina is finally able to see the blue smoke because it was signed, and in this case, in the skit we used little medals around somebody's neck, but that indicated the keys that are used to sign each level of the DNS tree.

So, next I'm going to turn over to my partner in this [inaudible] crime, Russ Mundy, who's going to talk about examples of why you need DNSSEC and some simple guides to actually deploying it.

RUSS MUNDY: Thanks, Wes. I'm Russ Mundy from Parsons, and the portion that I'm here to try to help you get a better understanding with is how you'd go about deploying it and what are some of the things you need to examine and think about as you go through the process.

So, one of the important aspects of DNS that many times people don't think about is that DNS is used by just about every application in the Internet today, and so when you don't get things right with your DNS or they're changed or for some reason there's a problem that occurs, a breakage or something, it's the applications that really hurt, that really end up with the problem. You can't get a connection. In the case of our skit, Joe User can't talk to his bank. So, that's the fundamental and broad across everything issue of what DNS is and what DNS does.

So, just as it's essential to make all the applications work, well, why do people go about attacking DNS? Well, I've been following the DNS and the DNS security activities for more years than I care to count, and frankly I have never seen or heard of an example where people attack the DNS because they want to change the DNS and just quit there and do nothing else. That's not what they're wanting to do.

What they want to do is they want to get access to information that's in some application that's running after the DNS queries have occurred. Maybe they want to just make a copy of all the email coming from a particular place, so they will, for all the destinations that that email server may be sending to, they could be sitting out there and giving the address for the falsified man in the middle type email server and receiving all the email that's coming out of that given machine, and then by the way, probably sending it on where it's intended to go and the people that receive it never know the difference. So, it's that type of man in the middle attack.

Now, a couple of years ago, and fortunately I did go back and look and see if I could find the courses again, and they at least don't appear to be out on the Internet like they were for a while, there were actually one or two courses where the instructors had in the syllabus the requirement for the students to write a DNS hijack. And in the syllabus there was nothing that I could see that said this is a bad thing to do, This is wrong. But there were also software packages out there that allow you to do the same thing. So, it's very easy to identify helping tools or existing software that's already out in the world. So, what is it that DNSSEC helps with?

Well, you then can know, as you saw in the skit, that the question that was asked by the user went through a process to verify the correctness of the origin of the information and the correctness of the content specifics that it wasn't changed in flight somewhere along the way.

So, this is an example of how some of the hijacks work. It's a somewhat simplified example, not quite as simplified as our skit, so let's go ahead and click the … You can see that's the first query, that dotted line coming from Joe User, and then it steps through to get the authoritative server, and then it comes back to the recursive server with the answer, then that goes back to the user, and then finally, after all of this occurs, the query actually goes to the web server. So, you can see there's a bunch of network traffic that happens that most people don't even think about – that's the DNS traffic that occurs before the web server traffic or email traffic or Facebook, or whatever you may be doing out there.

So, what we did a couple of years ago, we set up a customized site that actually will verify that the queries are coming in and are being DNSSEC validated and DNSSEC validation checks, and so what we did was there's a little X sign, a little check sign, and that was really just a custom done thing for this particular site, and then if you came in and did the same query and you weren't doing DNSSEC, you could see by the content on the page that in fact it was not DNSSEC verified.

What we did then was a DNS hijack that would show what could occur when this happened. So, go ahead and click first one goes out, next click. Dr. Evil, our wonderful helper here from the side with the big black cape, came swooping in and gave an answer, and that answer took Joe User off to the redirected website, and the query and answer that were the legitimate ones continued to pass through the system but Joe User and his machine never got it, because the first answer that he received, the one from the evil hijacker, had already come into his machine and the machine said, "Okay, got an answer, I'm not going to worry about anything else."

So, with DNSSEC, you get the same set of packet flows that you can see here, the difference being that with the validation check the packets that come and the DNS answers that come from the evil hijacker don't get accepted by Joe User's machine. I hope there were a few more [errors], but anyway, yes, those are the packets that just keep flowing their way in and out there.

Now, what is the custom web page look like? So, this customized web page looks just the same as it did when I showed it to you before, and now the next one . We did the hijack and in this case, this was actually when Steve Crocker was the chairman of the board of ICANN so that's why we – and Steve has been involved with DNSSEC for a long time, so we put a humorous link on another location that actually filled in a portion of the screen that the user saw if they came to that site without doing DNSSEC validation. So, we actually were hijacking our own information, in this case, just to demonstrate what could happen if there was an attack on a page like that.

Now, this is when you start with an empty resolver and an empty browser and go to cnn.com about 10 years ago. It was this thick. And today, it's considerably thicker. It looks more like that. So, this is just to fill a single web page. Next.

The important thing really in all of this, and the reason for doing DNSSEC, is to make sure that the DNS zone data, the zone content itself, is correct and stays correct as it's flowing through the Internet.

So, another very simple illustration, this is an unsigned zone, and doing the query and doing the answer … So, it's a small number of steps and it works very quickly all in the background. Then when you put DNSSEC in, whether you're operating the resolver and doing validation, if it's an ISP or a local enterprise, whether you're doing a large name server operation, you may be running a registrar and providing lots of name servers. Then if you're already able to run your own DNS systems, then incorporating DNSSEC into those systems should be relatively straightforward. The biggest challenge has been over time supporting the software to incorporate the DNSSEC capabilities, and that's very much improved in the last number of years, so most of the time you can get DNSSEC. If you're operating your own name servers, you just put the right software on.

Now, if you're a really large-scale operation, like a TLD or a very large enterprise, then probably you're going to want to be doing this yourself rather than having it outsourced somewhere. So, again, it's an extension of the capability that your organization probably already has.

Now, if you're an end user, then you, as an individual sitting in this room, you can be the person that's asking to have DNSSEC validation from your service provider, whether it's an enterprise, whether it's an ISP. In that case, you're probably not going to be running your own name servers – though a few a people do themselves – but most of the time someone else is operating it for it, and those operators are the ones that need to be asked to do DNSSEC validation to prevent Dr. Evil coming in and stealing your DNS information.

And, like I said before, the biggest focus of DNSSEC is to make sure that the zone data that is put in, in the beginning by the activity whether it's bigbank or whether its com, or whether it's another enterprise, is held in the system and delivered by the running DNS system to the end users and is not modified in the middle.

So, it's really the zone content that matters, and so that's what you really need to focus on – the zone content getting to the right place – and that is the as important as anything else … At one point there were a lot of people that were really focusing a lot – oh, DNSSEC uses crypto, that's crypto, and that's really special stuff, we have to do really special things. You need to make sure that your crypto is managed correctly and your keys are managed correctly, but most of the modern software do that. People need to remember you also need to manage your content correctly – getting it in and not having it modified along the way until it's in the name servers and then once it's in the name servers, using DNSSEC to validate it to get to the end.

So now, from the earlier pictures, there's not a big difference from the last block diagram. You can see it really is conceptually just adding some additional record types is what they're called in the DNS system, that are included from generating the zone that's contained in the authoritative name server, and then the validating recursive server validates that information, and that was the checking the medals as it went along as the ISP went down the row, from root to com to bigbank.

So, overall, as far as deploying things with DNSSEC, the important thing to look at is how much involvement does your organization or your particular entity have with operating your current DNS? If you're operating your current DNS in all the name servers and running them yourself, then you're probably going to be able to do those additional functions needed to provide DNSSEC signature and validation at the appropriate spots. If you're not operating it yourself – for instance, many large enterprises will outsource the DNS capability for their enterprise, happens to be parsons.com, uses an external provider like that. Well, one of the main reasons they chose the external provider that they did is that that external provider does DNSSEC.

So, if you're using an external provider you're probably going to want to ask that external provider to do DNSSEC for you, and don't be afraid to make the switch to another provider if the first one says, or your current one says, "Oh, I'm sorry, I didn't know you wanted DNSSEC; I can't do it." Find one that does. There's quite a few out there.

So, this activity is jointly hosted by ICANN and the Security and Stability Advisory Committee. We've also had some members from the Root Server System Advisory Committee helping us today, which is great, and the Internet Society Deploy360 Programme, so this is who we've had supporting these activities for a long time, and I think this is the last slide for us here. And then it is time for questions.

WES HARDAKER: Alright, thank you very much Russ. We're going to have Dr Evil run around down there amongst you all with a microphone, so if anybody has questions about how DNSSEC works or something that you didn't see in the information before, or you still have questions, please raise your hand and Andrew will walk around – sorry, Dr Evil will walk around and let you talk on the microphone.

ANGELA: Hello, my name is Angela. I'm from Botswana Communications Regulatory Authority. In the event that say the public key is hijacked by the hijacker, are there any mechanisms that are put in place to say, okay, in case the key is hijacked, how can I also verify if this is the correct response?

WES HARDAKER: That was an astoundingly good question. I'm not used to really good questions. Thank you for that. So, that's a great question. So, what happens if your key is compromised?

A couple of things there, and there's actually a lot of other experts in the room. Feel free you guys to raise your hand if you want to jump in and answer.

There's actually two keys that are involved, and we simplified it a lot, but there's actually a public key and a private key. You mentioned the public key. The public key you can give out to anybody. It's a safe thing to do. The purpose of public keys is that you can distribute them widely. It's the private key that you need to keep protected. If that becomes compromised, somebody hacks into your system and steals your private key, yes, you have to immediately tell your parent. So, if you are a bigbank.com, you would have to tell your parent, "I have a new key, please switch that chain."

Remember how the medals were checked all along? Basically, you would change one of those medals, you know, hanging on dot-com and say, "I have a new medal for you, I have a new key that I'm going to use. My private key is now different." And so, you can actually make that change fairly quickly. There's a lot of complexity that goes along with i. There's time to live values and caching and all sorts of other stuff that gets into play, but fundamentally, that's what you need to do. You tell your parent, "I have a new key. I need you to switch it immediately," and that keeps you fairly safe pretty quickly.

Any other questions? Good question, thank you.

SAVYO VINICIUS DE MORAIS: Hello, I'm Savyo from Brazil, NextGen. My question is about what's the biggest challenge that you are having to the DNSSEC the more used it in the Internet?

WES HARDAKER: So, the question is :what is the biggest challenge in getting more users to use it? Anybody want to answer that? I can take stab, but Russ?

RUSS MUNDY: Well, this has been a continuing effort in terms of both education, encouragement through various forums such as this, and the work that's been done by a number of activities to encourage software vendors to make sure they have all of the right structure and capabilities in their software, and working with application vendors to encourage them to also support it.

One of the, I believe, biggest helps for getting more people to use it comes exactly from users whether they're a user as an individual or they're a user that's part of an enterprise saying, "I want to do DNSSEC." Some of the registrar functionality at companies just don't do DNSSEC which makes it difficult then to get DNSSEC if you're using that company. Almost all of the registry operators now do handle it properly, but in terms of end users, end users can also ask software vendors that they use and increasing the demand and increasing the volume of the demand for DNSSEC is at this point probably the biggest motivation that folks need to hear because over time as various programs have directly approached these activities, the answer most of the time has been our customers are not asking for it, and so this is one of the reasons we do sessions like this, to help people not only understand what it is, but understand that you as an end user have a role, and that's to ask for it.

UNIDENTIFIED MALE: I'd like to add something to what Russ said. A few slides before the end, there was a diagram that had mentioned validating resolvers. When we measure the success of DNSSEC one of the metrics we use is how many zones are signed, but what's at least as important as that is who is validating? It doesn't help if you have all the domains in the world signed if the applications are not, if the recursive resolvers are not validating what they get. And then there was something else that I have for what you said but I can't remember, so I'll just shut my mic off.

WES HARDAKER: That's okay. So, good question, and we are constantly trying to collect statistics and track usage and see if DNSSEC is still growing, and if you look at deployment over time, DNSSEC itself is still growing. It's not growing as fast as we would like it to because it never is. As fast as we'd like it to would be everything assigned today.

This is a page I've put together. It's called stats.dnssec-tools.org. The data comes from somebody, Victor Duchovny, and he is an expert in tying DNSSEC to mail. As you can see, there's been a bunch of big jumps recently – very recently actually, in the past couple of months –that has tracked whether email servers are actually making use of DNSSEC signed email records. Some of those big jumps have actually come from recent companies that started turning on everything, all of their mail servers. They run more than one domain worth of mail servers, and they turned them all on at once, which is why there are big jumps.

So, the good news is that we are getting more and more usage, but a lot of its word of mount, a lot of it is activities like this and activities that the ISOC does to promote it. There's still a lot of work to do, even though we're over I think 10 million signed domains or something like that. The reality is that dot-com has many, many, many more than that so we're constantly trying to grow. Any other questions?

[COFY] My name's [Cofy], from the Ghana Domain Name Registry, and I have two quick questions. The first one is about the first question which is: is it a good standard practice to have private keys to be changed on a regular basis or to wait for it to get compromised before you effect the change? And the second one is: is DNSSEC a requirement for ICANN accreditation in any way, shape, or form for registrars and stuff like that?

WES HARDAKER: That's a good question. To answer your first one, there's two schools of thought on that. Some people believe that you don't need to rotate keys until it's compromised [the keys]. These days if you make them strong enough keys – because you can make very weak keys, but if you make strong enough keys you really don't need to roll them that frequently. I will tell you that I don't roll my keys that frequently.

The general guidance is that if you don't do it, you won't know how. So, operationally, if you do it on a regular basis, you can make sure that you have the skills you need in order to do it if you need to quickly, so a lot of people rotate their keys on a regular basis, once every year or something like that in order to do that.

The second question is that ICANN does have requirements for some of the bodies that they contract with. For example, all new gTLDs have to support DNSSEC. I don't know the answer to the registrar question. Do new registrars [inaudible] have to support DNSSEC?

RUSS MUNDY: I'm not certain, but I do not think the requirement is in a registrar requirement yet.

WES HARDAKER: Good question. Thank you. Other questions, there was one up here, and there's two in the back Andrew when you get done with them.

[CORY]: I'm [Cory] from the US. I had a question specifically related – DNSSEC's been around for a number of years as I understand it, but recently there's been talk about DNS over HTTPS or TLS, so how does that factor in with DNSSEC? Are they complementary, are they competing, how do they relate to one another?

WES HARDAKER: Good question. You guys are a very well-informed crowd. I'm impressed. So, there's a few things, and they're not competing. They're complementary in a lot of ways. DNSSEC signs the data, so it doesn't really matter how it's transported or where it's stored, it's sign so that you know that the record hasn't been altered. There is DNSSEC over TLS which is a recent specification that encrypts and authenticates the traffic between two devices. And DNS over HTTPS does the same thing, but sends it over HTTPS and the primary advantage of that is that it can't be blocked by firewalls that allow normal web traffic through.

So, there's different reasons for picking each of those technologies but the most important distinction between DNSSEC and the other two are that DNSSEC signs it so that no matter where you get it from you know it's authentic. You know it's been integrity protected. If you DNSSEC over TLS or over HTTPS you know that that single transaction is good but you don't have history of how they got that data.

So, DNS tends to use lots of multiple hops, lots of cases – like if you use DNS over HTTPS to go talk to one of the providers that do that, you don't know that they actually went out behind the scenes and got the right data and then checked it. Authoritative servers don't do DNS over TLS or HTTPS yet.

RUSS MUNDY: One quick plug for the Wednesday Workshop. There's a DNSSEC workshop on Wednesday, and there's a specific presentation in the workshop on that exact topic.

WES HARDAKER: Wednesday is a great day. If you want more DNSSEC, Wednesday's all about it.

RUSS MUNDY: Let me do a quick summary of what you said, that DNSSEC is there to protect the data. DNS over encrypted protocol is there to protect the privacy of your query, and they're two different things.

WES HARDAKER: Yes. Behind you Andrew. Way in the back next, okay.

[BALGISHNER]: Hi, this is [Balgishner] from Nepal. DNSSEC is protecting the end customer, right? So, is there any difficult to make the DNSSEC isn't mandatory, or maybe you can define the cutoff date and everybody needs to move to the DNSSEC – is there any difficulty?

WES HARDAKER: That's hard, because the world is a free world and people can choose to use or it or not. There is a common phrase: there is no Internet Police. There's nobody to enforce good versus evil in the Internet, so you have to pick technologies that work for you and make sure that you're using sites out in the world that might have it or things like that, so unfortunately, no, there's no way to force everybody to switch to using it. That would be so much easier wouldn't it, but no.

RUSS MUNDY: One comment is that some organizations have chosen to put security policies in place that dictate the use of certain security technologies. So, certain organizations have chosen to do that but there's no single answer for everything.

WES HARDAKER: That's a very valid point and there's certain governments that have chosen that all of their government infrastructure have to use DNSSEC for a good example. Thank you, that's a very good point.

UNIDENTIFIED MALE: Hi, I'm [inaudible] from Sri Lanka. I have on quick question. So, DNSSEC is disrupting the normal DNS flow. So, when this happens is there any slowing down of the Internet and if there is so, what kind of slowing down is there?

WES HARDAKER: Okay, so if I understand you correctly, you're worried about the speed that DNSSEC costs in order to do that validation. Excellent question. A couple of things. One, DNSSEC is a little bit slower because it actually requires a few more requests, and there are lots of studies. You can actually go find studies that people have actually measured that.

Here's the most critical thing. DNS data is cached, and I mentioned that once in the slide but we didn't talk about it very much. The security aspects are cached too, so once you go look up bigbank.com, all of those records have time links associated with how long your supposed to remember it. They don't go revalidate every time. Once they've validated it, they put it in their cache, they mark it as secure and then that's available for a long period of time. That's one of the wonderful features about DNS is that the first person that goes out maybe in the beginning of the day might have a slightly, barely measurable slower response, but everybody else after that gets the cached data so it's very fast. Good question.

[CHRISTIANNE]: Hi, my name is [Christiane] and I'm from Ivory Coast. I would like to know something – I'm not too technical so my question may sound a little bit stupid.

WES HARDAKER: No, no, that's okay, please.

[CHRISTIANNE]: But I would like to know, in the event of maybe a DNS being hijacked, is there any kind of procedures for the DNSSEC to resolve the problem, and has there been instances where maybe you have to violate those instances and maybe act directly?

WES HARDAKER: So, you hit upon a really hard problem that I think many security features in many protocols and even many physical systems. People don't protect their systems until it's too late.

So, essentially what your asking is once your house has been broken into and your money's been stolen, can you do anything about it about the fact? You can't. You've got to put better locks on your systems beforehand to protect it before something happens. So, DNSSEC can't fix things once you've been hacked by DNS. The good news is that hopefully in the same way that the caches will eventually expire, the bad information will eventually go away and hopefully your users will start getting the good information, but the reality is if you want to protect your DNS data today, you've got to deploy DNSSEC before you get hit by those problems. Does that make sense? Thank you.

ABRAHAM: My names is Abraham from Nigeria. My question is that in implementing DNSSEC, do we need to increase the hardware requirement of the system, or we need to maintain what we have before starting to implement it? Thank you.

WES HARDAKER: So, I think if I heard that correctly – I have a lot of echo, so I stand here next to this monitor. You're wondering if there's an increased hardware requirement for deploying DNSSEC. Is that correct? So, like more CPU and more memory, that type of thing? Yes, okay, good.

RUSS MUNDY: So, there have been a couple of different analyses done on this and mostly they have been done by people who are focused at the TLD or root level, and the quick conclusion was the normal growth and hardware replacement cycle that we're currently following is already sufficient.

However, what are the numbers? As I remember what they are, there's hardware impact of maybe 3 to 8% on your signing, but that's not real time. It's not done on … You sign before you load the zone. For validation, it's somewhere around that same level, maybe as much as 10%, but it's not a major impact but it is something that should be factored in as you look at your ongoing hardware upgrade program for your DNS infrastructure.

WES HARDAKER: Thank you. And the other thing to note is that there's a memory increase because there's more records and things like that. You do need a little bit more memory. So, as a case in point, I serve I think maybe 20 or so zones – I have never bought new hardware to deploy DNSSEC in any of the things that I've done. If you were a major TLD with lots and lots of entries, then you're probably going to have to consider but the reality is probably not for most people, that it'll run on your existing hardware without a problem.

[PAUL]: Hi, I'm [Paul] from UK. Are there any mechanisms put through by policy to track and monitor DNS breaches made to the TLDs or registers?

WES HARDAKER: To monitor for what purpose? We are here about DNSSEC today. Do you mean monitor for their security performance or the data that they're [distributing]?

[PAUL]: To build a database of breaches in order to, with the objective of flushing out the bad guys?

WES HARDAKER: So, it's very hard to monitor whether things are being misused because the reality is you end up having to monitor the whole world. I can monitor right next to the TLD and I can verify, hey, they're always distributing the right information but that's not usually where the attacks happen. The attacks happen [for your end users] and things like that, so you'd end up having to monitor every ISP in the world. That's a very complex question. Feel free to come back to me afterwards too if you want to talk about it further, because it's a hard problem and if we had the answer to that we'd certainly have caught all the bad guys by now.

UNIDENTIFIED MALE: Thanks. To add shortly to the previous answer about the hardware requirements of DNSSEC, a Network Information Centre in Czech Republic, nic.cz, is publishing regular benchmarks on DNS and DNSSEC servers. Just find me after. I will show you the link, so the impact on the hardware is negligible, it's just a bit, but you won't notice anything unless you're having your handling around a million queries per second on the single device.

WES HARDAKER: Alright, thank you very much. Andrew, down here.

[BRONWYN]: Hi, this is [Bronwyn] from Australia. My question is, so, in your skit earlier you had the resolver going and doing the validation of the certificate on each of the levels of the domain, so is there any updates or software changes required at the resolver level to actually support that extra validation because the resolver would be, I assume, doing resolutions for both DNSSEC enabled and non-enabled domains.

WES HARDAKER: Very good question. So, the good news is that most modern resolver software actually supports DNSSEC, like BIND and unbound are the two probably biggest ones. I don't remember the unbound version, but they've both supported every more important deployed DNSSEC feature for at least the last 5 or 10 years. So, if you're pulling anything recently or even distributed with any ISP server platform like an operating system, I can almost guarantee Windows resolvers do too at this point, so if you have anything recent it's really not a problem. It's been around long enough.

[CREJAN]: Hello, thank you. My name's [Crejan] from Nauru. I guess this is like DNSSEC for Dummies, so here's a dummy question. From an ISP perspective, are there any indicators or red flags that should be considered to indicate that DNSSEC is required?

WES HARDAKER: That's a very good question. So, ISPs are the ones that need to deploy a validator, that need to deploy – you saw my friend, Warren, walking around from person to person in the skit. They have to do the most work. They have to go talk to the root, they have to go talk to TLDs, they have to talk to servers for everything, and they need to make sure that their software is able to handle both secure and insecure look-ups because the reality is that until the entire world is secure you can't force DNSSEC to be on.

It's worth to note that we didn't talk about it during the slides and during the skit, but DNSSEC itself will tell you an answer of, "I am secure. This other server that your asking about is not secure, and I can verify for you that it's not so you're on your own at this point." So, there's actually techniques built in to do partial security and so that you can know when you get to the bottom that your either secure or you're not.

What ISPs should do is certainly monitor their logs and make sure, especially if they start seeing validation failures, that maybe something got attacked or maybe there's a problem on the Internet. Looking at logs is actually an important thing to do regardless of whether you're trying to deploy secure technologies or not.

[ALFIFA]: Hello, [Alfifa] from Bangladesh. I'm not sure if you're the right person to ask this answer.

WES HARDAKER: If I'm not, he is.

[ALFIFA]: The question was, if you have faced any major incident after a KSK rollover and how did you deal with that?

WES HARDAKER: Good question. So, the question, because it's going to lead into the DNSSEC workshop for you, is was there any issues after a KSK rollover, and what did you do about it and things like that?

RUSS MUNDY: Thank you. Sorry, I didn't hear it clearly. The acoustics are a little challenging here. Anyway, the event of the KSK rollover was in many people's estimation a non-event, and there have been some noted differences in the amount of traffic once the old key was revoked, but we're going to have a workshop session on that and there will be some information provided about that, and in reality from an operational perspective there was no really noticeable impact on the KSK roll at all. So, it was by all measures an operational success. It was a huge success.

WES HARDAKER: There's lots of back presentations you can go watch both on and previous DNSSEC workshops about why the KSK roll was delayed for a year, what some of things that were found. As I've given multiple presentations, a lot of other people have. And Wednesday, there will probably be maybe last set of presentations on that subject, because the revoked bit was just set on January 11th, and that was the last step in rolling the key and there is some interesting data that has come out of that, that's worth looking at. Come find me later if you actually want a list of URLs. I can send you videos to watch later if you're really that bored, but they're good. Any other questions? We have a little bit of time left.

Alright. I don't see any more hands so thank you all for such thoughtful questions. That was seriously one of the most informed audiences that I think that we've had yet. All of the questions were highly technical and it shows that you guys have done your homework ahead of time. There are no stupid questions. Please feel free to come ask me later if you want. All of this technology takes a long time to learn and we have been doing it for 10, 20-plus years, and so there is no such thing as a stupid question. There are only questions that you're just learning about and you have a lot to learn about.

A lot of us will be up here afterwards. Feel free to come talk to us. In the meantime, please enjoy the rest of ICANN and please come during the DNSSEC workshop on Wednesday if possible, because it's another great place to learn stuff, as well as Tech Day often is on Monday as well. Thank you very much.

[END OF TRANSCRIPTION]