ABU DHABI – Tech Day - part 1
Monday, October 30, 2017 – 10:30 to 12:00 GST
ICANN60 | Abu Dhabi, United Arab Emirates

EBERHARD LISSE: Good morning, everybody. If you can settle down. My name is Eberhard Lisse, I am the Chair of the Technical Working Group of the ccNSO, which organizes Tech Day usually on Mondays of each ICANN meeting. This time we have a quite interesting selection of presentations that I want to go through in the beginning.

We will first hear from the ccTLD administrator from the DNSSEC in the ccTLD. And also in the IDN so that's why the ccTLD is included.

Then we were supposed to change the name of the presenter on .tr DDoS attack follow-up. Not the problem but it's not Attila Ozgit presenting, it's Kadir Erdogan. That' not a problem in the final posted agenda, we will change the name with a link to the e-mail of the presenter if somebody wants to contact them, just go to the website and click on the link.

Then we will hear about some IDN staff in e-mail addressing which I don't understand and so Dimitri Belyavsky will explain it to us. And then the Saudi Telecom DNS revamp will be presented.

Then at 12:00, we break for lunch. We didn't find a sponsor, we didn't look for one. So it's self-catered as usual.

Then in the afternoon, Francisco Arias from ICANN staff will explain the RDAP Pilot. As you all know, RDAP is the upcoming replacement of the WHOIS. And they're looking for guinea pigs or volunteers to participate in the pilot.

Then we will hear original presentation about the DNS operations of Etisalat. Then Francisco Arias will talk about the EBERO test. I think it's the emergency backend registry of last resort type of thing. And we had a test in London I think. That was one where one gLTD was given back so the use is to test this and they did another test and he will report it.

Akkerhuis will speak about the root canaries with measurements in that they started to implement to measure the impact of any of the KSK rollover. And then Arends will explain to us why the key is not being rollovered just yet.

Then we have the usual host presentation. We always ask a local ccTLD manager or the audit organizers to give a presentation of the topic of their choice. We haven't heard from the host recently so if Al Marzouqi is in the room, can you please raise a hand? But we are trying to contact him. We can always move his presentation a little bit further back if there is a contact issue.

Then Jack will talk about some – it's called Home Network Registry but he is basically about Internet of Things and from the DNS perspective, local perspective, he will talk about it. It sounds quite good.

Then being in an Arabic script region, IDN is always a topic of interest. And then Google will present something about HSTS which I also don't understand very well. But Ben McIlwain one of our members who works for Google presented this presentation and the consensus was that it might be interesting.

Finally, .CN will talk about the issues of registering names in an IDN and an ASCII domain at the same time to keep consistency and coherency.

The closing remarks will be done as usual and this time by Norm Ritchie. Norm Ritchie was recently appointed to the SSR2 Team. The Security and Safety Review Team 2 which has recently undergone some stress points. It appears the Board is having second thoughts about the way this is going on. So he can maybe give us some quick words about it.

Some housekeeping, we have a remote participation. We present from Adobe Connect software which is visible on the outside so if there is a question coming from the remote participation, they will go to Kim. Kim will raise a hand when

there is question time and we will try to take the remote questions with a priority unless we overlook them.

That is all. I have to say, which means we can start with the first presentation which would be DNSSEC in Saudi ccTLD. Let me hand over the [baton].

RAED ALFAYEZ: [inaudible]. Welcome, everyone. I would like to thank the organizers for giving me this opportunity to present the Saudi Arabia experience in deploying DNSSEC in the Saudi domain names. My name is Raed Alfayez, I am the Director of SaudiNIC. I have so many slides. I will try to squeeze them and maybe jump some of them.

This is my agenda. I will go over the role of SaudiNIC/CITC. And managing Saudi domain names. And what we have done regarding DNSSEC and most importantly is what are the lessons learned that we have learned from our experience in our domain.

So CITC represented by SaudiNIC/CITC is the Communication and Information Technology Commission in Saudi Arabia which regulates the ICT sector. And SaudiNIC is the ccTLD manager for .sa ccTLDs and .saudi in Arabic language, the TLD for all the country in Saudi Arabia. We manage as usual as any ccTLD

registry. We develop the policy. We run the operation. We also coordinate with international bodies regarding Arabic domain names and Saudi domain names.

Most importantly is the last one. We develop and operate the Saudi ccTLD infrastructure. And what we mean by that is we have 24/7 resolving service. So we make sure the resolving for the .sa in the Saudi TLDs are going as expected. And we do protection for the infrastructure.

Here are the most important items that we have done on how to protect our infrastructure. So we have hidden primary DNS servers. As usual we have two copies hosted of them main servers at CITC premises. And we have three hosted within Saudi Arabia, one at ISU Internet Service Unit in King Abdulaziz City for Science and Technology and two with our partner STC company. It's one of the biggest telecom provider in Saudi Arabia. And we have two external providers that provide Anycast service with around 150 Anycast nodes.

The last mile that we have done in this protection area is we enable DNSSEC and .sa and .saudi. It was officially this year but as a pilot project last year. So what we have done, we were putting eyes on the DNSSEC topic and technology. And we were monitoring RFCs. We are learning from other mistakes so we are just collecting information and waiting for the maturity for the

RFCs and the application and the monitoring system to be available.

At 2015, we started the second phase, which is the study phase. So we have done base market with some countries. And we learned from them. And we have done a study on how we are going to approach the DNSSEC. And after that, the study ended with having three stages. So the first stage is getting and building local expertise within SaudiNIC and CITC and within the kingdom of Saudi Arabia. The second stage was having a prototype as experimental operation and the final stage is going live and launching of the actual DNSSEC service.

So our strategy was to step by step methodology. So we don't rush. We learn. We focus on what are the mistakes that have been done by others. And why we have waited that long? Actually we waited for the tools and applications to be mature so we got a little bit bug-free systems and applications and monitoring tools as possible. And we waited for some of the RFCs NSEC, NSEC3. Something just to get more mature because we don't want to – we are not a leader in this area but we want to go and go slowly and make sure that everything should go as expected.

And again the percentage of global use within the ccTLD industry was less than 2%. So it's a little bit low, that's why we

have no rush. So what we have done, we have started with a study, a comprehensive study, and we have done benchmark with some of the leaders in this area like Netherlands, New Zealand, Canada, Australia, Austria. And we have done benchmarking about lots of things. What are the policies, what are the technical parameters that they are using? So we just have a complete picture of how to deploy DNSSEC.

So the study as I told you, it has three stages. And Stage I is gaining and building local expertise. Stage II is prototype and experimental operation. Stage III launching the actual operation.

What we focus more, we focus on building local expertise. So we need to have Saudi citizens, Saudi engineers have knowledge on DNSSEC. And we have done good building a good relationship with some outside expertise. We shared with them some of the issues that we are facing or it was difficult for us to understand. And we depended on open source tools and softwares.

So this is some of the training and workshop that we have conducted. So with the first training was done on October 2015. It was a 3-day course. It was aimed for CITC and SaudiNIC employees and for local some of the important government agencies and the local telecom providers and operators. The second one was done in May 2017 this year. It was a 2-day

course and we have expanded. The first one has only 25 participants. The second one training has 41 participants from 29 government agencies and ICT operators including ISPs.

And we have one public day event. So it was – we asked all government, all security agencies, all banks come and to know about DNSSEC, what is the use of it. And we have done all of these with some of our partners like RIPE and [MENOG] and ICANN. This is images from the first and second training. And this is some images of the workshop and we handled certificate from the training in the same workshop the public day.

So these are some of the deliverables that we have done. The first one was the SaudiNIC DPS, DNSSEC practice statement, and we believe any registry that want to operate, they should have something like this. And this is an example. We have it publicly and we publish it in Doha language. So we are the first one to have it in both Arabic and English. And we try to make the translation not a literal translation but it's in the meaning, mainly in the meaning. It was difficult to translate KSK, ZSK, these technical terms. But we believe that we have done a good job there.

So we have done DNSSEC setup and they will show it to you. And we have done procedures or how to maintain and manage DSSEC keys. We have DSSEC credential matrix so it says who

should do what and who'll have the keys, who'll have the case code, who'll have the passwords. And this is explained exactly if someone leaves, what things that he need to hands on or what things need to be changed. And we have done a DNSSEC risk management so if in case of failure for the hardware security module, what will be there if there's a failure in the sign or machine, what would be there? So it's a set of procedures.

This is the DNSSEC setup. It's a little bit – seems to be complicated but it's very easy. Actually we have only two sites. So we have DNSSEC room, we call it room and all the keys, so many things happening there. The second one is a backup for it. We have safes so we stored the keys in the safes and no one leaves the room – no one enters or leaves unless he signed the attendee list for the one itself. Then the keys will be published through private network to the signer machine and then the signer machine will sign the zone file from the database and then publish it to the Hidden Master. The Hidden Master publish it then to the global name servers that are reachable all over the world. And then it will be distributed to our secondaries.

These are set of procedures that we have built. We have the DNSSEC Key Generation Ceremony. It's a detailed script having each step from entering the room until you leave the room. And generating the key, how to start them, who does what, etc. And we have the procedure for Key Installation Procedure. We have

procedure for emergency Key Installation Procedures. Also a procedure for New Safe Arrangement Procedure, and for the Safe Content Transfer Procedure. So everything have procedures and it is audited by our internal auditor at CITC.

So in June 2016, we were the first DCC country to enable DNSSEC on our .saudi ccTLDs. And we give the operator the chance to go on registered domain name and enable DNSSEC, play with it, make sure everything is okay. And once they are ready, then we can do it in the production environment.

In June this year, we have enabled it officially in .saudi and TLDs and we are the first in the Middle East region to do this one, to enable it, and enable for our customers. We conducted the Key Generation Ceremony. We signed the .sa and .saudi. We published the key to IANA. We updated registration system and staff accepting DS records from our customers. We have done awareness and promotion.

And we have a website. It's called www.dnssec.ca. That's in two languages, Arabic and English. It's explained to you what are DNSSEC in Doha language, what are the keys, what are the KSK, ZSK, what are the rollovers? Some of the technologies behind the scene, we try to explain it as we could. And hopefully it will be someone else will benefit from it, either from Saudi Arabia or

from outside Saudi Arabia on how to know what's DNSSEC and how to use it, how to deploy it.

This is some pictures from the Key Generation Ceremony. It was a closed room and these are our colleagues that has participated in all. They have signed on that Key Ceremony Script that has everything. These are some of the tools that we have allowed, published for our customer to test their DS record before submitting it to us. So this is the DS verifier. DNSKEY Record Information and then it will verify if they are a match or not before they submit it to us.

This tool called the DS Record Generator, it has the domain name and DNS key and it can fit it from your zone file. And then it can generate the DS for you if you don't know how to generate it. And this tool has been built by my colleague, [inaudible] he's in the back. He's one of the experts we just hire and he just put him in the DNSSEC area and he started reading RFCs and implementing tools. So thank you, [inaudible].

So what are the lessons learned? Okay, this is the most important thing. You need to build local expertise. It's difficult to depend on outside expertise so we need to have local people reading and knowing about DNSSEC. You need to have test lab to test the systems or software that you are doing to implement or build and to test the parameters for the DNSSEC. So what's

the relation between TTL and key signature lifetime, and what are the relation between the barometers for the DNSSEC? These all need to be done in test lab before you go live in production. You need to develop monitoring and testing tools for the DNSSEC systems and your zone files. Monitor your zone files. Don't publish your zone file unless it passed some kind of tests, so test the zone file is not broken. The signatures are valid. Lots of tests before you publish it. Because if you publish it, you lose. So you need to have some monitoring and testing tools to validate the signed zones before publishing them.

You need to have automation for most or some of the key generation ceremony procedures. And the ceremony if you want to create the keys, you need to make it as automatic as possible because otherwise we might have some human errors and redo the ceremony again.

You need to provide customer support because believe me, users may get confused with DNSSEC. It's difficult for them to grasp. It was difficult for us it will be more difficult for end users to grasp DNSSEC, what's the relation between DNS key DS – what's the different flags in the DNSSEC record and DNS keys? So we need to have tools to help the user to validate his work before submitting a DS record to the registry.

I believe our next step will be more awareness and more promotion. We need to monitor and enhance the DNS protocols. So we monitor the enhancement and the DNS protocol. We have that NSEC file is coming so we need to keep an eye on what's new in DNSSEC.

Also the most important thing as a registry, we need to keep an eye on the key rollovers. We have a lifetime for the keys and every six months or one year, a rollover will happen. And we have built it in a way to be automated. But again, we need to monitor it and make sure everything is okay.

This is some statistics so we have above 50k domain names registered under all of our TLDs. Until yesterday we have 55 domain names enabled, DNSSEC enabled, so 33 under .sa directory and 8 under .saudi the IDN for our Saudi country. And .com.sa was 6. .net the same, 1 .org and 1 .gov. And we are negotiating with [.sr] which is the Ministry of Information and Technology to enable – to let's say mostly recommend the first stage for a government agency to enable DNSSEC. And then another stage it will be enforcement for them to have DNSSEC enabled in their system.

That's it and thank you for your listening.

EBERHARD LISSE: Thank you very much. Several things I liked very much about this presentation in particular I like the way that both languages Arabic and English were on the same slide. That looked very cool I must say. The appearance of the presentation was very, very nice I must way. You have the same issues and the same solutions for the same things that we all have. Documenting, automate procedures that you can automate because if tab something, you have to do it all over.

The other thing is I see you have the uptake is very slow. My question is what are you doing about getting the resolvers to resolve your – it's an all-or-nothing thing because you must force all the servers in the country to resolve. Otherwise, the ones who don't have a competitive advantage, what's your plan in that – do you have a plan or what's the plan in that?

RAED ALFAYEZ: Yes. Since 2016, so last year we started gradually with our partners like telecom providers and ISPs in Saudi Arabia and we sent them like letters asking them to be prepared for DNSSEC to make sure that there is resolver have DNSSEC enabled. Also with regards to the latest thing that happened with the rollover for the root, we also send them, asking them to update their resolver software and make sure they have the new keys. So CITC is the regulator for ICT in Saudi Arabia and we have direct

relations with our partners telecom providers, DSN providers and ISPs.

And the relation is strong and we are exchanging, having meetings, and we have direct contact like our colleagues from CITC. And they have hosted two of our secondary name servers in their premises, one in two cities in Kingdom of Saudi Arabia and we thank them for that. And we are still forcing other telecom providers to have a secondary and make sure their resolver is DNSSEC aware and can resolve things in the best way to do. CITC have today a speech about the infrastructure and their readiness and maybe you'll hear more about that from them.

EBERHARD LISSE: Any questions from the remote audience? From the floor? Okay, thank you very much. Give him another hand please. Okay our next presentation is a follow-up on the DDoS attack on .tr done by Kadir Erdogan. We had this I think two or three ICANN meetings back I don't remember exactly which one, Attila Ozgit gave us a presentation about what happened during the DDoS attack on Turkey, on .tr a few years back. So we're very grateful that they volunteered a follow-up presentation. And let's go with it without further ado.

KADIR ERDOGAN: Hi, this is Kadir Erdogan from .tr ccTLD. I am the Technical Manager. I will try to give you a brief information about the DDoS attack we had on December 2015.

This picture describes what happened there. As you can see, if you can fill all the roads, it is almost impossible to the destination. And this is true for the Internet too. If you can fill all the lines, all the pipes, for the packets to reach to their destination is almost impossible. You can even stop the Internet too.

Before the DDoS, everything was great for us. We were having infrequent small scale DDoS and DoS attacks. It was easy to mitigate them. We had six name servers at five different locations at three different ISPs. We were running Bind mainly. And Bind were running only Linux servers. Our average bandwith was 1.5 megabyte per second per server. As you see, it is nothing. Since we are running automatic name servers, it is normal. All the heavy load is done by the recursive name server. So life was good for us.

There are three major ISPs in Turkey each connected to Tier-1 at various locations. Four of our name servers were located at 1 ISP. One name server was located at another ISP and one name server was located at Europe.

This is the anatomy of the DDoS attack that we had. You see that is the attacker. That is the botnet. There are lots of servers, public servers. And at the end, the nic.tr DNS servers, the victim. botnet is a network having lots of computers, baby cams, DVRs, that kind of connected devices. And those devices are mostly hacked or maybe they're running some malicious software. And the target servers, not the victims, but the servers are public servers. They are mostly running UDP-based services. And some old services, old protocols. DNS is one of them. DNS is really an old protocol.

And how does it happen? Attack sends a comment to the botnet to start the attack and the computers or the devices at the botnet sends queries to the target servers. Mostly they are spoofed UDP packets. And the target servers who receives the query thinks that he should reply to the victim because of spoofed UDP packets.

This is reflection. And since the response size is way more than the query size, you have an amplification too. This attack is called reflection and amplification attack. If the used public servers are DNS servers, then you have DNS reflection and amplification attack. If the public servers are NTP servers, then you have NTP reflection and amplification attack.

The attack started at Monday morning, December 14, 2015. It is really strange for me to have an attack on Monday morning because if you are the technical people, most of the attacks starts at Friday afternoon. We don't know why they did this.

EBERHARD LISSE: They unionized.

KADIR ERDOGAN: Basically, it was a DNS reflection and amplification attack but they have used all UDP protocols, almost all of them. An interesting number is that the attacking IP addresses were from Turkey mostly. Not mostly but 25% of them. It means that we were attacking ourselves as the country. The target was mainly our six name servers. But after that, they have tried some things or our web-based services, TCP services too. They have tried as well injections towards our WHOIS server, for instance. They have tried for many place and then web-based attacks too.

There was two kind of attacks at that time. At the working hours, they were sending us big data packets with amplifications to saturate lines because at working hours, you know people are utilizing the lines. So it is easy to saturate the lines, to fill all the lines at working hours. But when it finishes at non-working

hours, they were not sending big data packets but they were sending very small but too many packets.

The target was networking devices and our name servers. They were trying to do bypassing the memory limits of network devices with packet per second, many large packet per second numbers. We actually don't know the exact picture of the attack. But we have a number from one ISP reported. It was 220 gigabyte per second bandwidth from our ISP and it might be one of the largest DDoS attacks at that time.

If you are having an attack, your basic reflection is increasing the number of name servers. And maybe modifying some configurations. Maybe relocating some name servers. What you have to do is you have to analyze your traffic. You have to figure out drop rules to be used by the network operators because network operators know the network. But they don't know much about DNS. What they understand from DDoS mitigation is to drop all the packets. And if you are running an authoritative name server, it is the worst thing to do.

We have some observations. As I told you, measure attack was UDP flooding. They were spoofing the packets. We have seen a major pattern. It was Source Port 53 and Destination Port 53. This is actually an old habit of old DNS servers – but not anymore. So if you see this kind of pattern, it is probably an

attack. They have tried almost all known attack patterns in the book. We have seen also some web-based attacks too as I told you. We analyzed our database. We took all the name servers registered to our database and we checked them. And 8% of them were "open resolvers." It is horrible actually. It shouldn't be.

About UDP flooding, I can say that technically it is easy to prevent it. If you – not you, of course – if you are the ccTLD managers, you cannot do that. But the network operators can do this. If they implement ingress and egress filtering in their network devices, then we wouldn't have this problem.

At the attacking time, as I told you, you will want to change your name servers. You will add more. You may want to reconfigure them. And the step to do it is RZM. RZM is Root Zone Management system. It is run by IANA ICANN. At that time IANA transition was not finished. We were having delays, days of delays for the updates. And most delayed step was DOC checks. DOC is the Department of Commerce of USA. And it is not applicable anymore because of IANA transition. You may want an effective communication mechanism between your technical team. You can use some Near Real Time Chat technologies like Whatsapp. It's a good idea because your phone is not in the network of your infrastructure so it will be continuous.

You can use your own system. We are doing that. You may want to talk with your upstream operators before the attacks. Know them, meet them.

The critical communication should be in written form. It is important because at the attack time, your technical team or your whole team is anxious. They are sleepless. They are angry. And that feeling, it is not easy to express yourself on the phone. A small mistake, a small misunderstanding on the phone may cause way more than the attack itself. So all the critical communications should be in written form.

And of course, since they are attacking through your DNS infrastructure, your communication channel should be tolerant to the DNS failures.

You may want to talk to IANA ICANN folks. Meet them before having the attack. They are very helpful. Nice guys. You may want to talk to other ccTLDs. There is a mailing list for the ccTLDs for this kind of [stations]. You will probably want to talk to other organizations within your country like your national CERT. You will want the press of course. You will want your upstream operators too.

Just after the attack, we were having infrequent, relatively light DDoS attacks. And we are still having them. We took some administrative measures at that time. We have created a list of

critical domain names. First day it was 100 of them. A few days later, it became more than 1000 domain names. Mostly government domain names and banks, etc. For instance, Google.tr was one of them.

We have temporarily decreased daily number of zone updates. We were manually inspecting all the zone updates because we were afraid of having a problem, having intrusion in our registered services because during the DDoS attack, we were focused on the DDoS. So we might be missing some bad things happening in our web system, web-based application system. That is why we are very keen on inspecting zone updates.

And currently we have eight name servers, two of them are ANYCAST from DynDNS. 12 name servers for second level zones, com.tr, gov.tr, etc. Three of them are ANYCAST, PCH and Dym. With ANYCAST we have more than 100 DNS servers around the world. We have an isolated zone creation system. There are some locked critical names. It is not possible to update them through our web interface. We have some automated security checks over zones.

We have some manual security checks done by humans. Of course we are not checking all the domain names but we are just checking all the critical domain names. And we are running multiple hidden master servers. Before the attack, we had one

single master server and it was public. It is bad. It was definitely bad.

That's all. Thank you.

EBERHARD LISSE: Thank you very much. I think this is very good that we can hear follow-up of these things. We have had reports about DDoS attacks and this is the first time we actually had a follow-up after a few months or year time so that you have time to correlate your analysis into a proper report type of thing that you can then report back to us. Any questions?

One thing I saw somebody take a photo of the presentation. That is not necessary. You're more than welcome to it I'm just saying the presentations will all go on the websites so you can all download them after the fact if you want to.

Any questions? Sorry, all questions must go to the microphone because the remote audience can't hear it.

UNIDENTIFIED MALE: This is [Hamil] [inaudible] from STC. I would like to ask did you try any kind of DDoS mitigation techniques like purchase any equipment from some vendors who's doing DDoS mitigation or subscribe with any scrubbing center where you can redirect your

traffic there? I saw that you just increased the – use ANYCAST, using ANYCAST is a very smart idea. And increasing the number of servers but still I think using the DDoS mitigation vendors or scrubbing center is a smart idea also. And I'd like to see your point of view of this.

KADIR ERDOGAN: Actually, as the ccTLD manager, it is not something you can do. But the network operators can do. Of course we had some mitigations over network operators. But we didn't have control over that mitigations. That is why communication is important because network operators doesn't know the nature of the attack. We were reporting to them, filter this out, filter this out. And they were taking their mitigation services. And it was happening. But it was difficult because they should do that, not us. Because we are not network operators.

UNIDENTIFIED MALE: Yes, sure. But later on for now, I mean for now…

KADIR EDROGAN: Yeah. We have some DDoS mitigation services. But they are services and those services are not in control of us. They are controlled by the network operators that we have some name services.

UNIDENTIFIED MALE: Thank you.

EBERHAR LATISSE: Can you identify yourselves for the audiences please.

SIMON JOHNSON: Sure. My name is Simon Johnson. I am a Board member and a Director of ADA responsible for the Australian ccTLD. My question is, in relation to the effects of the DDoS in your country, what did you observe? What was the practical impact that this had in your space? Was it slowing resolution, availability? What did the general public and the government say?

KADIR EDROGAN: We have noticed the DDoS. But the public didn't notice it much because of the running authoritative DNS servers, actually. [Thanks] to [TTS] and recursive DNS servers. The public didn't know much about the DDoS attack. But of course we were having problems like we were having problems for zone updates, zone transfers because our master name servers was one of the public name servers and it was under DDoS attack. So the other secondary name servers couldn't be able to take the zones.

The queries were a bit late. But again, our traffic, our regular traffic was 1.5 Megabyte per second. They are not asking to us directly. People not asking queries to us directly. We are running authoritative name servers. So the public didn't know much about it.

SIMON JOHNSON: Could I just ask a follow-up question?

EBERHARD LISSE: Take your time.

SIMON JOHNSON: So if I may, the general public in using your Internet or if I'm connected to an ISP, would I notice anything at all? Would it slow down or if I registered a domain name, it might not get updated?

KADIR ERDOGAN: It was not much noticeable by the public. They have learned the attack two or three days later by the media. But again, thanks to [TTS].

AFIFA: [inaudible]. Afifa from Bangladesh. Second time Fellow. So I work in a daily com operator in a cybersecurity analyst as a cybersecurity analyst. My question was, if I consider that my service is down due to DDoS attack and I have no tool in place right on that moment, so how will I be necessarily identified that this service is down due to DDoS attack? I mean how can I identify right on that moment because it can be down for any other reason, anything can be happen right on that moment.

And the second question is, even if I have identified, I will not have enough time to analyze my traffic as it is impacting my revenue. I have the pressure to keep my service up. So apart from analyzing the traffic, what can be done right on that moment instantly?

KADIR ERDOGAN: Actually, it depends on the services you are giving. I can't talk about the DNS servers. You have to monitor your servers. And you have to monitor your servers regular bandwidth usage, lots of CPUs, lots of things. If you see some peaks, you can create some notifications for your technical team so that they can analyze before it goes high. It may be something regular but we have to monitor. This is the rule.

I don't know how to monitor every services. That should be some customized specific monitoring. Everything's for the

services of course. If you are monitoring some web servers, it changes. If you are monitoring some DNS servers, it changes. So I don't know the exact response to that.

EBERHARD LISSE: The short answer is Anycast. PCH.

KADIR EDROGAN: For the DNS, yes, Anycast.

EBERHARD LISSE: PCH and others do this for free. They are around over at Martin-Legene is probably in the audience. James Mitchell was in the audience. People are sitting around. You can talk to them if you don't use them. Especially small ccTLDs in developing countries will find it very easy to get free Anycast services. We have got redundant Anycast services when we had an attack again as we asked one of them, can you tell us where it's coming from? No, we didn't notice. We can't specify by country, we can only do it by continent. And it's so small. And our infrastructure, we didn't notice. That's what you want to hear from your Anycast provider.

We also some presentation a few years ago in Singapore where Steven [inaudible] and I spoke about attacks against our servers

and you can look at this packet queue. You can look at what's coming into your wire, you can analyze this. But on the other hand, you gained so much data so quickly that it overwhelms normal databases like MySQL or PostgreSQL. And then you need to go invest into big database where you don't have to know. The short answer is Anycast. If you don't have it, go to PCH immediately and talk to them whether they're willing to help you and they are.

AFIFA: Thank you.

EBERHARD LISSE: All right. It was a very cool presentation. Thank you very much. And I also like the questions that were coming from the audience. They were also quite helpful, to be honest. Next is Dimitri Belyavsky will explain to us what EAI in X.501 means.

DIMITRI BELYAVSKY: Hello. My name is Dimitri Belyavsky. I will tell you about newly appeared specifications regarding using the Internet internationalized e-mail addresses in X.509 certificates. Not a problem.

Here is the brief history of standardizing of the e-mail address international list. It began in 2007 and was finished for most e-mail protocols in 2013. Here is the list of RFCs specifying the SMTP extension. And using it in SMTP protocol, mailing list in IMAP, in POP3 protocol. And some other related standards.

For now, international e-mail addresses are more or less worldwide data. There are a lot of mail services supporting international e-mail addresses. A lot of mail clan support it. Large mail providers including Google Gmail provides support for e-mail address. And according to our Russian-based statistical project stat zone, about 1.3% of MX-servers and 2.6% of domain zones are solved on the servers which we flag as STMPUTF8 on that. This flag indicates that support of international e-mail addresses.

But as e-mail addresses are widely used in all the protocols, there are a lot of places where we still need to provide centralization of using international e-mail address with the same roles as we use as e-mail address.

For the main industry, we should name the EPP protocol which currently doesn't allow international e-mail address although there are some experiments, for example, I know that in Thailand, it's allowed to use internationalized e-mail addresses in WHOIS. There are not finished standards of using e-mail

addresses internationalized in X.509 standards. I will speak about it. And of course, there are some other places where we should add specification of internationalized e-mail addresses. So if you know please add them to list.

Currently, support of e-mail address internationalized is discussed in ETF in working group named Lamps. It's acronym, I don't remember how it's full title. And it discovered by two drafts which are near to becoming a standards. The first one is written by Russ Housley. And the second one is written by Alexey Melnikov and Weihaw Chuang. Here are the links to their working group itself and to the drafts and I will say some more words about each document.

The first one named Internationalization Updates to RFC 5280 is in fact a set of patches to RFC 5280 which is X.509 and CRL profile. So it specifies how to use non-ASCII e-mail addresses in certificates. It requires IDNA 2008 compatibility. I believe it says checking that provided their IDNs are valid. It specifies using A-labels anywhere but non-ASCII e-mails. I will speak about it when describing the next document. And it specifies using their host name in SmtpUTF8 mailbox which specify their presentation of non-ASCII mails.

So if we have ASCII local part, then hostname should be A-label and for non-ASCII local part, the hostname should be U-Label.

This document also reference to there are draft related to internationalized e-mail addresses in X.509 certificates which is a separate document. This document contains the following specifications. Of course more and more but here I've written the most significant ones.

First, SmtpUTF8Mailbox is a separate possible value in general name field of certificates. It's an extension of an operation of other name field. Then this document specifies the rules of comparison of e-mails when we check if their certificate match the e-mail address. And the most significant part of this document is about applying name constraints. So this document specify that name constraints limiting on the local-part should not be used. That we need to apply the domain-level name constraints according to rules specified in RFC 5280. And that CAs must use RFC – the classic ASCII e-mail address for subject [with alternative] names.

When this document was published, we tried to make an implementation of it. For now, we have a preliminary version of the patch implementing this document in OpenSSL. Here are the link. It's a preliminary version. When it was finished and was published upon request, it had unpredictable result for me because the authors of OpenSSL, the OpenSSL core team reviewed not only the patch but the document itself. And it

caused a process to change the document more or less significantly.

The patch provided depends on LibIDN, which does not fit the current open cell policy. So it needs to be revoked in this area at least with providing IDN encoder decoder in open cell core. The patch of course needs more testing. And the documents are not finalized. Some OIDs that should be included in this patch are to be finalized too.

So if anybody is interested, I would like to discuss the testing and the adopting this patch, well feel free to contact me today and tomorrow. Thank you very much. If you have questions, please e-mail to this address. No, I don't have non-ASCII e-mail mailbox. So please feel free to contact me. Thank you.

EBERHARD LISSE: Any questions? All right, thank you very much. And now, for the unenviable last presentation before lunch. We will hear about Saudi telecoms DNS revamp.

ABDULAZIZ ALAQIL: Good morning, everybody. My name is Abudalaziz Alaqil, IP Design Manager at STC Saudi Telecom. First of all, I would like to thank ICANN for giving us this opportunity to highlight the effort that we've done in revamping our DNS infrastructure.

During the session, I will take you through briefly about STC Vision 2020 and the DNS types that we have in our infrastructure. Then we will talk about our recursive DNS revamp and authoritative DNS modernization. Then I will conclude by highlighting our initiatives and our future plans.

Beginning of this year, STC has launched its 2020 vision that resulted into a strategy that aim to prepare the infrastructure for the new telecom servers generation that will require high-speed, low-latency, high-density like 5G and IOT. These services will result into a security risk and it will bring a security risk and more threats. So it was mandatory to draw the security strategy side by side with the services strategy. Security strategy covered multiple domains. One of the domains that we covered in our security strategy is DNS. So securing that critical surface and make it available is one of our targets.

In the STC, we have four main DNS types. We have recursive DNS. Our recursive DNS serving more than 20,000,000 customers from both mobile and fixed. The second type of DNs that we have is authoritative. We are hosting more than 1500 customer zones. The third DNS type that we have is we have multiple copies of ccTLD or Saudi TLD servers. The third type that we have is ICANN root servers. We have multiple instances of multiple copies of ICANN root server.

STC recursive DNS, it is a very critical service. So in our strategy we focused into securing that very important service and make it available for our customer to sustain the customer experience especially when it comes to DNS because it's one of the Internet enablers and the most targeted services by attackers.

So from security perspective, we implement multiple techniques and solution to protect both our customers and DNS infrastructure. We protected our customers from spam and malware by evolving and implementing solution for anti-spam and anti-malware.

For our DNS infrastructure, we implement multiple solution to mitigate the most known DNS threats like denied of service, data corruption, DNS fraud, and the other types of DNS threats. For our DDoS mitigation plans, we are protecting our DNS infrastructure from both volumetric and doublication attacks and to contribute also in globally spread of DNSSEC. We have enabled DNSSEC validation in our recursive DNS.

From the availability and capacity point of view, we have enhanced the performance of our DNS infrastructure, our DNS recusive can handle now more than 3,000,000 query per second. And it is distributed into four sites. From the availability point of view, we have three level of redundancy, we have local, city, and region redundancy. And we have implement the Anycast

solution to load share and load balance the DNS request on network level.

For our authoritative DNS, we focused into securing that service. We are actually implementing currently the DNSSEC. It will be available for our customer within [inaudible]. We have implemented Tsig protocol to secure or authenticate the update between our authoritative servers. And in addition to that, we have implement DNS or DDoS application mitigation mechanism in our authoritative DNS. And from the performance, we have enhanced our performance and we have authoritative performance. And the redundancy, we have make it up to two levels.

Our initiatives, we believe in our national role as a national provider or national operators to enhance the Internet experience for Saudi citizens and STC customers. So we have adopted multiple initiatives to enhance that service. We are hosting multiple copies of a root ICANN server to enhance the Internet experience for our customers and to contribute in global availability of L-root servers. Also, we have did the same for Saudi TLD. We are hosting multiple covers of Saudi TLD server to contribute in its availability and to enhance the STC customer experience.

Our future plan, we will continue focusing on securing the DNS and our future plan forecast to secure the downstream traffic between end user and DNS servers by implementing DNS over list to protect the customer privacy. In addition to that, we are going to implement HSM solution. That solution into manage our customers' DNSSEC keys.

That was a brief about what we did in revamping our DNS infrastructure and the drivers behind it. Thank you very much. Any questions?

EBERHARD LISSE: Thank you very much. Also very nice presentation and well delivered. I must say thank you very much. Any questions?

ABDULAZIZ ALAQIL: They decided to take early break.

EBERHARD LISSE: You must come to the microphone please because our remote audience needs to listen.

SAIF AHMED: Hi. Thank you for the presentation. This is Saif Ahmed, Head of .iq department in Iraq. Please could you give more information

about your application for DDoS mitigation that you mentioned at your presentation?

ABDULAZIZ ALAQIL: Yeah. Actually, we implemented the DDoS obligation mitigation by analyzing the traffic and analyzing the requests that will come to our DNS recursive and based on the behavior of that request, we are doing either to drop the traffic or rate limit the request from the requester.

SAIF AHMED: So it's automated or you're monitoring?

ABDULAZIZ ALAQIL: Automated.

SAIF AHMED: Okay, thank you.

EBERHARD LISSE: Anything from the remote audience? Thank you very much for an excellent presentation and give him another hand. I am now going to release you to lunch a little bit earlier than expected. We meet at half past 1:00 and then we have a relatively packed program until 5:00. Thank you.

[END OF TRANSCRIPTION]