CLAUDIA RUIZ: Good morning, good afternoon, good evening to you all. Welcome to the LACRALO monthly call on April the 18th 2022 or 230:0 UTC.

on Spanish we have Augusto Ho, Alfredo Lopez, Carlos Aguirre, Gerardo Martinez, Gilberto Lara, Hannah Frank, Harold Arcos, Laura Margolis, Rodrigo Saucedo, Sergio Salinas Porto, and Vrickson Acosta.

We have Claire Craig on the English Channel and Sindy Obed in the French channel.

We have received apologies from Sylvia Herlein Leite and Dev Anand Teelucksingh.

On behalf of the staff we have with us Silvia Vivanco and myself on call management today.

Our interpreters today are and Marian and Paula on Spanish, Esperanza and Bettina for the Portuguese channel, and Jacques and Claire for the French channel.

We also have with us Alberto Soto who has just joined the call.

Before starting, I would like to kindly remind you to say your name before taking the floor for interpretation purposes and I'll give the floor now to Augusto.

AUGUSTO HO: Good morning, good afternoon, good evening. First of all, let me begin by thanking you for joining the monthly call for April. And I wish you all

the best for today's discussion. Welcome. And I'm going to give the floor to Claire for her to go over the agenda so that we can adopt it. Go ahead, Claire.

CLAIRE CRAIG: Thank you, Augusto. Welcome, everyone to our monthly LACRALO call. Today, on our agenda, we have the pleasure of hearing, Nicolas Antoniello who will be speaking to us on how we make DNS more resilient and secure. And please note that this is the first of two parts of this webinar. So we look forward to this part. So get your questions lined up for Nicolas.

Then we have a short report from the Board which will be delivered by León Sanchez. We also have another report from our ALAC representative Carlos Aguirre, and another exciting project that is happening we will be hearing from Sergio Salinas Porto who will be giving us an update on the planning that is taking place for the LAC digital project that is coming up in May.

Under our regional updates, we hope to get a report from our regional representatives. But we also have to talk to you a little bit about our elections for 2022. At this point, I would like to find out from you if there any other items that you would like to have discussed under any other business. Please raise your hand if there is anything.

Okay, I'm not seeing any hands raised at this point in time. So I take it that we are agreeing to this agenda and it is passed for this meeting. Okay, so I turn the meeting back over to Augusto. Thank you very much.

AUGUSTO HO: Thank you, Claire. As mentioned by Claire, on our agenda today we are having a very exciting presentation delivered by Nicolas Antoniello. We will have approximately 45 minutes to talk about how we can make DNS more resilient and secure. So let me welcome Nicolas Antoniello. You have the floor.

NICOLAS ANTONIELLO: Thank you, Augusto. First of all, let me thank you for inviting me to address you all today and to talk about this topic. So those of you who don't know me, I'm Nicolas Antoniello. I work at ICANN as a regional manager for Latin America and the Caribbean region, technical engagement. And the plan for today, we're going to have a discussion on the DNS as a whole, and its extensions, and the standardized protocols that have been added to the basic DNS protocol in order to make it more secure, and also more resilient overall.

And as we will see, in some cases, there have been privacy functionalities that have been added to DNS. I'm talking here specifically about data privacy and privacy for queries entered by users. So let me share my screen.

Yes. So we are going to talk about how to make the DNS more resilient and secure. At any point during my presentation, if you have any questions, any comments, just let me know. You don't need to wait until I finish my presentation. In fact, I think that presentations are more entertaining if we have questions in the middle of the presentation. I will not be paying attention to the chat. So please, Claudia, let me know

if there are any questions coming through the chat or if somebody wants to take the floor. So don't be shy, ask all the questions or make comments along the presentation.

Okay, let's start now. The first slide seems to be missing something because it is blank. Basically, you have here the snapshot of the web browser that is blank. But what I wanted to illustrate here is that, as you well know today, when you want to access a website, on the Internet, before the browser can download all the components for a certain site that you are trying to access, we need to enter an IP address that will connect to the servers that will enable the system to download all the necessary components to access that website.

And as you may know, we do not have just one single server. Of course there is one main server but today, you can get information from 10 or 20 different servers, so you need to make queries to several servers in order to have authentication components in order to retrieve text.

So in order to display a website, and to access a website, you need to make several queries into the DNS. Usually, we have the name, the domain name that is part of the URL, and you need to have access to the IP address in order to retrieve the page. That is where the DNS plays a critical role. And the query at the user level is like a blind query, the user doesn’t know what is happening.

The user cannot see what is happening on the user side, the computer or the mobile phone will have access to the recursive server that will be in charge of making the query against that IP address that the user is entering. So the query will be sent to the DNS and the associated

servers and search will take place there starting from that IP address. And then the DNS is going to bring me back and answer and the browser or the app that is being used will be able to execute all the remaining actions. In the case of a website, user will be able to access that website and will be able to see all the content displayed.

But that is hidden for the user, the user doesn't know that all that process is taking place. And the user today cannot be sure whether the IP address is the correct one. So, sometimes if there is an attack that is perpetuated on a certain address and can always change and alter that IP address that is received by the client, the web client is going to access the site thinking that it might be the reliable site when actually it may be a fraudulent or malicious place that can give you false response and it will [lead] to maliciously set up site.

Some elements that we need to take into consideration when we are using the system, when we are trying to use the Internet, we have e-mail services, calendar services, contact services, the contact book is always on the Internet, if you have a problem with your mobile phone and you want to share that contact list so that contract work, you will have it stored somewhere in a cloud online. It is not simply stored on the mobile phone.

Then you can have database services, business data, customer data in the case of organizations or companies we work for, employee data, stock data, file servers that contain financial information or internal documents of the company, service that also stores processes and procedures, we can also have control and operation systems like equipment control or monitoring systems, service provider. We are not

just talking about Internet service providers, we can also talk about energy supplies or water suppliers and all of them use monitoring systems. And at a given point if they have some contact point with the Internet, these systems can be accessible from the outside or can be remotely operated.

Then you may also have provisioning system, you may have control access systems, password systems, then VPN, different security mechanisms and other types of systems.

I tried to apply some common sense here on this slide and throughout the presentation, you will see several examples. In Uruguay, we usually say that sometimes common sense is the least common of all the senses. So we need to train our common sense. Things that may seem to be common sense may not be that evident for other people. So you need to be well informed and trained in order to know what the potential threats and risks may be and what are the options to solve those, to overcome those risks or to mitigate them if you cannot solve them.

So, all these elements that are already online usually have as a starting point a DNS query. That is the starting point. So, quick review. DNS is a distributed system in terms of the way the information is stored, that information is not stored in one single server all over the world, it is distributed across different servers and information is not concentrated in one single organization.

There are several organizations that take care of the distributed management and administration of all those servers. These

administrative divisions in the domain name space are called zones. So one administrator for one zone manages one part of the DNS system.

A zone manager can also delegate the management of [subtrees] below these zones. So, the DNS structure or architecture is an inverted tree structure. So you have the roots, then the branches, and then successive trees. And leaves in that tree may allow the manager to delegate those zones.

And then we have two types of servers. We have recursive servers and authoritative servers. And here the name in Spanish is not the correct one. So we have authoritative servers and recursive servers. The authoritative servers store information for each zone and for each domain. And the recursive servers are the ones that retrieve or run the search for the information in the domain name system on behalf of the client. It is not the device itself that runs the search. The device provides the query to the recursive server, the recursive server runs the search and then it comes back with a response to the client.

Why are we going through all this information? This is just a quick chart to show you the DNS resolution mechanism. We are going to skip this and we are going over all this because from now onward, the presentation is going to delve into different aspects of this entire DNS mechanism. We are going to see the different threats that are the most common ones, where they usually take place and what are the resolution mechanisms, what are the ways to avoid those threats entirely, or when that is not possible, when the threat cannot be avoided or eliminated, how they can be mitigated using protocols or any available procedures.

When we talk about threats, we will usually refer to these three types of threats. They are not the only one but they are the most common. Phishing, that is a fraudulent practice of sending e-mails, messages pretending to come from companies or known services. This is just to deceive individuals. Phishing targets users so that users will think that they are actually accessing a certain site or a certain service, when actually the goal is to make that user reveal personal information, passwords, credit card numbers, among other details in order to use that personal information in order to retrieve information or to inject information into a system or to have a non-authorized access into a system in the case of passwords for instance, to access users' bank accounts to steal from or to commit fraud.

Then we have malware, what do we mean by malware? Malware is not targeted at users but devices, this is software that is specifically designed to disturb the function of a device or to cause damage to that device perhaps on a temporary or permanent basis or perhaps not to disturb, not to cause damage but to obtain non authorized access to an IT system or to a device in order to extract that information. So if I want to get information from a site and I am an attacker, I will try to do it silently without anybody noticing it. So I will try to get unauthorized access to all those areas so that I can extract that information. And if they learned that that access has taken place, that should happen quite late. These are some examples, ransomware, key loggers, rootkit, viruses, etc.

And then we have botnets. Botnets, are also aimed at devices, not users. But what do we mean by botnet? It is a network of private computers. As an attacker, I will set up that network and I will use this

network of computers at web to commit an attack on a third party later on, so I will prepare all those devices, I will inject malware, malicious software into those devices without the user knowing that. And when in the future, I want to release a distributed attack, for instance, I will send a command to all those devices, I can be talking about thousands of devices that are compromised on the planet, so I will send a command to those devices so that the software gets activated and all those computers will act at the same time against a user. For instance, they may send data, a lot of data to third parties. If it is just one device, that will not be a problem. But if we have hundreds of thousands of devices sending data against a third party, probably that third party will have that denial of service type of attack, and that third party will not be able to continue providing the service because it will run out of bandwidth. There are many more sophisticated attacks using botnets.

Why do we talk about threats to or against the domain name system? Because we all use it. So it's very appealing to attackers to make it vulnerable, or to attack some other system. If I'm able to disrupt the DNS system, I'm actually shutting down the Internet. Because as we said at the beginning, everything starts with an IP query. We do not remember the actual names. If I'm disrupting this protocol, I'm interrupting all commercial transactions actually everything of the region where the attack is being conducted, social media, government and nongovernmental organizations, everything can be troublesome, or in some cases catastrophic. For example, an attack on a health care system, energy, drinking water can be actually catastrophic.

And by exploiting the DNS, we can also commit fraud against users such as stealing credentials for bank access. Some attack vectors we can

mention are the most widely known ones are registering domain names maliciously. This happened a lot during the pandemic, specific domain names were registered pretending that there was information on COVID vaccines and people accessed these sites. And they were actually accessing information on COVID vaccines, but they were in addition to downloading a file, users were also downloading malicious software, malware. So they were injecting in the user device malicious software.

The name resolution or registration services hijacking, this is an attack on domain name owners, alteration of DNS data, modification of information, data collection through compromised websites. That could be on any website to engage them in compromised user data collection.

And DNS service data extraction, this is a little bit more technical, we will have to [inaudible] talk about how attacks operate. But this is an attack basically that uses a well-known port, 53, to extract data. And it uses the same channel as a mechanism to extract data on the organization, because organizations have typically to leave this port open because it's the DNS gateway. If they close it, they cannot resolve the DNS and attackers can use this DNS functionality to extract the data and bypass the firewalls and whatever security measures organizations have.

This is nice. What you can see here is an outline of the entire DNS ecosystem, including registries, registrars, users. Here where you read stub, stub is the DNS software that the client runs on the device that sends the query to the recursive resolver, which in turn looks up among authoritative resolvers. And then we have the registry through the registrars and the rest of the DNS system.

So here, the red crosses, the Xes show several points where an attacker might commit some sort of attack. So these are the points where potential attackers can commit attacks. So what we're going to see now is a description of some mechanisms introduced into DNS to operate at these points and either prevent the attacks or mitigate the attacks when the attacks cannot be addressed.

The sad reality is that this is an endless race. Attackers are always motivated to find new vulnerabilities and new vulnerabilities will always rise up because people make mistakes and the more complex the software is, the more possibilities for attacks. There is virtually no comprehensive software error free. So vulnerabilities show up. Can be repaired, but there is a time between repair and error when vulnerabilities appear.

Attackers are increasingly creative and at times highly sophisticated. There is a no hero here, attackers are always a step ahead. And what we can do is either implement some prevention measures, with as many prevention measures implemented, or react. When an intrusion is detected, either it is addressed or mitigated. And I should learn from that, and do some research and see if there is any mechanism that I can implements for additional prevention.

So there is always some new mechanism. So we will always see new attack vectors coming up. Some mechanisms to solve, mitigate for potential implementation. Let's see. The first one we're going to talk about is this thing of maintaining multiple alternative servers. What is it?

Imagine I have the authority for a certain domain name, my domain name is Nicolas.com. I do not have it. But if I had it, let's take it [inaudible] and I implement my DNS server for my domain. And I have the zone file for Nicolas.com with all the data of my sub domains. For example, I have a laboratory.Nicolas.com, documents.Nicolas.com, www.Nicolas.com for my website, etc.

So I maintain the Nicolas.com. This zone can be stored in different servers. I can either have it in just one authoritative server that is easier, or, which we're talking about here, instead of having one server, have several, all of them identical, all with the same information, they will all have the entire data for my zone, Nicolas.com.

What is the advantage here? Whenever a recursive server anywhere in the world tries to resolve the IP address of any of my domains, Nicolas.com, they will be able to query any of the copies I have of the authoritative server. Why is that? Because they all have the same data.

So instead of having all the data in only one server, I have several with the data replicated. That is called zone replication. And this fortunately has existed since the very beginning of the DNS standardization as a mechanism by which any server you choose, any application, BIND, [Knot,] whatever application you may choose, PowerDNS, BIND, any of the applications for authoritative DNS already implemented this feature, zone replication, and the DNS protocol supports it.

So it's relatively easy to create several servers and afterwards, activate this protocol feature so that every server has all the data. I execute any change, any modification in one server, and the rest will be in sync. And

they all will all have the same copy as the data stored in the server I have defined as the main one.

What is the advantage behind this? Whenever there is an attack on one server, I will know if there is a failure or an attack, I will not be out of service, because there will be other servers providing the same services. If I have too many queries, or if anyone decides to carry out an attack by an extensive number of queries, what I can do is distribute the query load among the many servers so I have a greater response capability and I'm more able to mitigate a high number of queries that may come up.

So somehow, I'm making the system more resilient. There is another technique, Anycast, that can also be used. And I am going to talk about it exactly after describing the replication, because in order to have several authoritative servers—there may be other options, but the standard thing is to implement it in one of the two following ways.

One of the ways to have several servers for the same zone is that when a domain name is delegated to a subdomain, at the parent level, in order to set up the child for the delegation to take place, a DNS record is created that stipulates the name of the authoritative servers for that delegated domain name.

And I can list several server names. So whenever a recursive server is looking up for that information, and asks me which is the authoritative server for this, I can give just one name if I have only one registered, or the list of names, as many as I have entered, and the recursive server will try to reach any of them.

All of them will have the same information because they will all be copies. So a recursive queries one and that one does not respond, it will go on the list. So I can have a list with names of servers that are actually copies. That's one way.

The other way is Anycast. The Anycast technique, the difference, Anycast is defined as a combination of IP addressing and routing, whereby the decision on which is the destination of the package is taken by the network routing mechanism. Basically, it doesn't require any special configuration at any level. The only thing it requires is that the same IP address is assigned to many devices.

The authoritative servers do not have any more different names, but they will both have the same IP addresses. You may wonder how is access carried out. It doesn't matter, because actually all of them are copies of the same. So they all keep the same information, it doesn't matter which one I'm accessing. All of them, or any of them is able to provide the same answer. So this is a case when I can assign the same IP address to two different servers, because all of them have the same information. If all the servers have different information, and I assign the same IP address, that’s a problem. But this is not the case. That's what the Anycast technique consists of, several authoritative servers with all of them with the same IP address, and whenever a query is made, the network and routing will decide to which the package will be sent, and the answer and the reply made.

So I'm implementing the same mechanism but in a different way. What are the advantages, the benefits of Anycast? Well, it provides redundancy and resiliency, it distributes the query load, as we've seen

before, it distributes the query load, and the load of answers amongst many servers. As I was saying, it reduces the latency because all of them have the same IP addresses and I could go to those copies that are closer to the clients. So the time in between the query and the reply will be shorter. And that reduces the latency and name resolution is faster. And eventually providing a greater strength to the system. And I contribute to mitigate events of denial of service or distributed attacks, in this case, against the DNS infrastructure.

So this technique can be applied both to authoritative servers and to recursive servers. I can have several recursive servers and use the same Anycast technique. We're not going to talk about implementation now, because that'd be for a different webinar. It requires knowledge on routing, etc., we can go for that later on.

In case of implementing this technique in authoritative servers, it is very important to consider that all of them must have exactly the same information. But the good thing here is that DNS protocol already considers this. And there is a mechanism to maintain this zone with an indefinite number of servers. That's already implemented, the root server copies.

This is a different way to provide resilience to the domain name system, which involves the not the entire DNS system, but just the root, the root of the domain name system. You know that the DNS root is where the tree starts, that DNS tree.

The DNS root, being overly simplistic, we could say that the owner or the manager of the data contained in the DNS root is ICANN, is IANA as

ICANN's centralized office, but it's not ICANN, the one that serves the public. ICANN manages the information but does not serve it. It is provided by the maintainers, the organizations that maintain authoritative servers.

How many of these organizations do we have nowadays? 12 organizations which you see here listed. Actually, the list is 13 but you see that A and J is the same organization, Verisign. So even though here you see 13 letters, actually, they are 12 organizations, each one of these 12 manages one root server organization.

We have actually hundreds of servers for each of them, because each organization through the Anycast technique assigns the same IP address to several servers and that is how they create several copies each and maintain several copies of their root server.

This is site rootservers.org that shows through a map an updated list of the root servers all over the world. This is a snapshot I made today on the website. And the value is absolutely accurate. According to this website, as of today, there are 1533 instances or copies of the authoritative root server. So these 1533 copies of the root zone, some are managed by one of these 12 organizations.

You see that in our region, we have 29 in the North America, which also comprises the south of the Caribbean, 29 instances of root servers, approximately 110 copies in South America, and 266 you see in United states. There are a few that correspond to the north of Caribbean. As you see, there are several hundreds of copies in Latin America and the Caribbean for the root servers, these root server operators.

So in this way, we for the DNS root where that is the starting point for the query, we can have several copies. So someone who is a recursive server will start the search and can access any of these copies. So since there are a lot of copies, and they are close to the client, these provide more resilience, more error tolerance, less latency, more prevention of attacks, and higher service quality for users when resolving domain names.

So with this program that exists through ICANN and other organizations that are the ones who manage and maintain the service for the root zone, we can apply and maintain and install a copy close to the users in your own country or in your own region. So that is another way of increasing, enhancing the resilience and the security of the DNS security.

Are there any questions so far? Am I going too fast? Are we doing okay with time?

SILVIA VIVANCO: Yes. We are doing fine. I don't see any questions. Only one comment. I can share it with you privately so that you can have a look at that.

NICOLAS ANTONIELLO: Okay, so let's continue. DNSSEC. This is a DNS security extension, that is the name. And this has been decided in order to improve the security of the DNS. So it is called DNSSEC. So as you may recall, we had the ecosystem, the global DNS ecosystem. So DNSSEC has a role here between the recursive and the authoritative server. Remember that the

stub resolver will send that query to the recursive server, that recursive servers will send the query to several authoritative servers starting with the root one, and then response will come back.

So that communication between the recursive and the authoritative server can be improved from the point of view of security with the DNSSEC. So the players that have to deploy the DNSSEC protocols, those that manage recursive servers and those that manage authoritative servers. So this happens between these two types of servers, not with a client. So DNSSEC is handled by recursive and authoritative server [inaudible].

So what does DNSSEC do? It uses public key cryptography and sometime in the future, we will speak in more detail about this. And it also provides digital signatures in order to have authentication at the point of origin. That means when you send a query to the recursive server and to the authoritative server, you get a reply from the authoritative server, the authentication at the point of origin enables me to know to be sure that that reply really came from the authoritative server that is capable of providing that answer, not from an attacker or a fraudulent place. That allows me to make sure that the information is reliable and it is coming from the server with the right authority to provide that [inaudible].

And in addition to authentication, DNSSEC provides data integrity. So while data was traveling from the recursive to the authoritative server, that means that the data have not been modified. Does DNSSEC prevent modification of the data? No, but if data has been modified, and I have DNSSEC in place, then I will be able to know that that modification of

data has happened, I will be able to tell whether they have not been modified. And if I do have origin authentication, then I can rest assured that that will be reliable information.

If I'm accessing my bank's website, the query is run against that DNS. If there is no DNSSEC protocol in place, I will never know as the customer of that bank whether I am really accessing that true website of their bank. There is no way of knowing whether the data has been modified. So the attacker may set up a page that looks identical to my bank's website. So when I enter my password, then the attacker will get my username and my password if DNSSEC is deployed when the query is sent from the recursive servers to the authoritative servers.

If the reply is authenticated, the recursive server will realize whether that is reliable information or not. And the user will be able to say that the recursive service has realized that false information was being retrieved. So the DNSSEC protocol prevents that kind of attack. So it offers protection against DNS data that is not reliable, and it also avoids cache poisoning attacks.

So data is encrypted when traveling so there is no confidentiality feature in DNSSEC and it cannot prevent denial of service attacks. But it can assure you whether the data has been manipulated or not, it does not encrypt data.

So what are the technical benefits of DNSSEC? it provides authentication as we have already said. It guarantees data integrity and non-manipulation. And DNSSEC also provides you with a mechanism that tells the client what has happened if the query is run against a

nonexistent website. I will get an answer through DNSSEC. And how can I know whether the problem is that the site does not exist or somebody has falsified that information? DNSSEC has a mechanism for the authoritative server of that nonexistent domain to tell the recursive server that that domain name does not exist and confirm that it does not exist, and so the client or researchers that that is actually the case, that that website does not exist, that is not [inaudible] or they are pretending that the site does not exist.

These are the technical benefits, but there are also benefits on different parts of the ecosystem. For the end users, it gives the user the confidence that that person will get to the desired website. From the registrant standpoint, it also mitigates fraud. It provides more trademark protection concerns considering that [country code] reputation from the point of view of the registrar—it ensures that it complies with industry standards, and it can meet the demands of registrants for higher levels of security.

And this allows registrars to attract and retain registrants because they care about security and reputation. And for the registries, these days, it guarantees that they are complying with the best industry practices, and that they can fulfill the demands of registrars.

SILVIA VIVANCO: Nicolas, I'm sorry to interrupt you but we are running out of time. And I would like to read a couple of questions that Alejandro Pisanty has written in the chat, because we only have half an hour left for the rest of the call.

NICOLAS ANTONIELLO: Yes. So I'm going to leave the rest of this presentation for the second part of this webinar, if you agree. So what comes next? [inaudible] on different mechanisms and we can see this on a different call.

SILVIA VIVANCO: Yes. That sounds great, Nicolas. We will have a follow up webinar. This is very interesting. So let me read the questions. DNSSEC used to have a non-desirable side effect that was to facilitate the publication of entire zones. How will that be mitigated at present?

The second question is, from which size onwards would it be cost effective for a manager to implement DNSSEC given the cost and the complexity? Thank you.

NICOLAS ANTONIELLO: Thank you, Alejandro, for your questions. Because in your first question, let me read them again, the non-desired side effect of DNSSEC that is, it allowed you to sweep across the zone. If I understand your question correctly, Alejandro, and for others to be able to understand, so it is true that with this mechanism, DNSSEC can give me the confidence that the website that I'm looking for does not exist.

But during the first few deployments of this protocol, the protocol in particular is called NSEC. And that portion of the protocols in the first few implementations, the first few deployments, this is true, they enabled attackers with certain level of ease to run several queries and

sweep across zones, and somehow find out which domains existed and which ones did not exist.

One simple example would be just to go over the dictionary and look at all the different words in the dictionary and start running queries against those words in the dictionary to see if there are domain names associated with those words.

So when there is no website, you're also going to get positive answer telling you that the website does not exist. And the same happens when the website exists. And that will allow you to have access to all of that without copying the entire information.

There is another extension now, DNSSEC 3 that changes the behavior of the protocol when there is no zone. So it makes it almost impossible for attackers to sweep across all those zones and obtain that information. But of course, that will depend on the extension that is being implemented. If it is DNSSEC or NSEC 3. But that applies to obtain information from all the sources.

Sometimes we are too careful and registries that manage authoritative servers are careful not to disclose information. But the files are public, because otherwise the queries will not be able to be resolved. So this fact of being able to have access to an entire zone does not necessarily imply that that will present a security problem.

It may be a problem because you may be getting a list of clients from a certain record. And that may be a security issue for a registry. That does not imply a security risk for the user or for the domain name system. Of

course, it is a valid concern for registries and registrars. But it is not a security issue or an important security issue.

There are a lot of—for instance, in the case of the root zone that is public, you have a lot of files that are public, and they can be downloaded publicly. And some of the zones are public, and that is part of the business of registries or registrars.

But my answer to your question is that with DNSSEC 3, that problem is mitigated, it makes it so difficult for attackers that they cannot get that information.

And the second question was about the size from which for a manager, it will be cost effective to implement DNSSEC. We talked about recursive and authoritative servers. If you just deployed for recursive service, that will not be helpful. If you just deployed the protocol for authoritative service, that will not be useful. You have to deploy it on both.

There is almost no technical overload when you deploy it for both types of server. So today, if you installed a recursive server, any recursive server software out of the 10 most common ones already have DNSSEC enabled by default. So that already gives you an idea of the low level of complexity that DNSSEC brings about.

For people who have had servers for many years perhaps to activate now DNSSEC would not imply the technical overload. Perhaps they have to add some more memory. But DNSSEC does not overload the server. This is almost negligible considering the benefits that you will get in terms of number of customers, number of clients.

But you always have to monitor the protocol, no protocol can be left on its own, you always have to keep some level of monitoring. Now on the authoritative side, the complexity is higher because you need to maintain the signature, you'll need to have the activated keys, you'll need to implement some maintenance mechanism. They can be more or less expensive depending on the level of critical role of those servers.

If I'm a ccTLD managers, every day I can have dozens or hundreds of new domains and I will have to sign them. And I need to have DNSSEC enabled for them. So I need an online automated mechanism so that when a new domain name is created, automatically that signature should be created. That is not impossible. That is not so typical nowadays.

We have a lot of support. There is a lot of experience. A lot of people have been doing this for years. And there is also a big supply of training, affordable training.

Now taking advantage of your question, Alejandro, at ICANN, one of the things that we do is to invite and encourage operators to contact us. And we offer them support throughout the deployment process for DNSSEC, both on the recursive and the authoritative servers.

Of course, we can provide them with support, even if they are private operators. We are not going to tell them what they have to buy but we are going to train them so that they can get on board and they can operate with a reasonable level of efficiency. Of course, on the authoritative side, it implies perhaps higher costs. But that has more to do with training.

So about DNSSEC, what I can say, in a nutshell, is that DNSSEC should be implemented by everyone, because it solves a very important problem. And if that problem takes place without the protocols, the user will not be able to tell them.

SILVIA VIVANCO: I see some hands raised by Carlos and Sergio, but we are running out of time, Nicolas. So Nicolas, if you agree, we will stop now with this part and we would like you to come back once or twice—apologies to Sergio and Carlos. Because we are running out of time, we need to continue with the next agenda items. Perhaps Carlos and Sergio, if you have any specific questions about this presentation, you can send it to me or to the rest of the staff in writing and we will forward them to Nicolas.

NICOLAS ANTONIELLO: Thank you. Yeah. Of course, if you just send me the questions, and I will reply them and I vow to go over those questions and those answers in the next call.

SILVIA VIVANCO: Thank you. And apologies to all of you who raised your hands. Augusto, please continue with the next agenda item.

AUGUSTO HO: Thank you, Silvia. I want to thank Nicolas for his participation and his commitment to follow up on the topic with the several questions. So

now let's move on with our agenda. Now, we need to give the floor to León Sanchez. He is going to report on the ICANN Board activities

LEÓN SANCHEZ: Thank you. Good morning, good afternoon, good evening to you all. The Board has been quite active lately. Over the last few months, as you know, we had our Board workshop before the ICANN 73 meeting and we have had different interactions with the community during ICANN 73 itself.

We started our workshop on March the 1st and we went over the strategic trends analysis. This enables us to [sense] the ecosystem to try to anticipate what issues may crop up that require our attention by the Board or by ICANN Org and the level of participation that ICANN needs to have in these different areas. So we analyze trends that may seem non relevant to all, all the way to those areas of issues that may pose some risks to the organization.

By way of example, I can mention the alternative domain name resolution systems that are appearing now with blockchains systems and some other alternative systems. We try to examine the impact on the current DNS, how we should carry out this discussion, whether we need to interact with those that are proponents of these alternative domain name systems. This is just an example of the different trends that were considered during our workshop.

We also had a session during which we looked at the different activities with governments and intergovernmental organizations within the ICANN ecosystem, the different initiatives that are taking place in

different countries, mainly in the European Union and the potential impact that this may have on ICANN's activities.

On the second day of our workshops, we talked about DNS abuse. And we also discussed the outstanding recommendations from the SSR2 review. And we also talked about the proposals to defer the SSR3 review.

The Board came up with a resolution to postpone the third SSR review in order to be in line with the ATRT3 recommendations. There was a specific recommendation from the ATRT3 review team indicating that the next review of SSR should be postponed until all the ATRT recommendations are implemented. So we halted that review, and of course, we will have to wait for the next version of the ATRT.

We also had another session with Göran Marby. We talked about the DNS threat mitigation system. And he also presented a report on DNS abuse. So we also dedicated some time to looking at how we can prioritize the different activities that are on the Board's plate right now, trying to align this with the community's priorities.

And, of course, the Board needs to engage in many activities. So we need to set some priorities based on the level of urgency, the resource allocation, the relevance for the work that we need to do. So we usually have this kind of analysis and during this exercise, we try to make sure that this will not be just a unilateral listing by the Board, we just want to make sure that the list of priorities that we establish in the Board can also have some input from the community. We want the community to tell us whether they agree or not with our priorities. So we tried to look

at all the different components within ICANN as an organization. The Board is just one more component that needs to have a say in this prioritization exercise.

On the last day of our workshop, we looked at the results, the outcome of the Operational Design Phase for the next round. And we looked at the results of the evolution of the ODP, consider a future round of new gTLDs and then we had our regular Board meeting, adopting different resolutions.

One of them as I have already said was to postpone the SSR3 review. We also adopted resolutions for the Phase 2A of the EPDP report from the GNSO Council and we also submitted for Board consideration one resolution regarding an independent review process, an IRP process involving the .web gTLD. There was a controversy. There was a dispute among different stakeholders that participated in the auction to get this new gTLD delegated.

As a result of this dispute, and conflict of interest that arose, there was a litigation process. The case was not taking to court per se but we had to apply the corresponding rules to this case. So the independent review process was started to deal with this case.

The panel has already issued its recommendation and the resolution was submitted to the Board consideration and the Board resolved that the [BMC,] that is the Accountability Review Committee has to review this decision and come up with recommendations for the Board. So the process is not over yet. It will continue. It has to be examined by this committee.

And another resolution that I'm sure that you are already aware of is the one that has to do with the establishment of an emergency fund to provide support for ongoing access to the Internet. Of course, this is part of the fallout of the crisis in Ukraine given the conflict that exists in the region, so the Board decided to allocate $1 million to this fund so that work can be done with people in the region to secure ongoing access to the Internet in the region of the conflict. Of course, fulfilling ICANN's mission and properly managing the funds.

So Augusto, basically this is a quick summary of the work done by the Board and in the next few weeks, we will meet in LA for the first time in person after a long time of virtual meetings. we will meet with leaders of the different supporting organizations and advisory committees and we will meet the Board as a whole. It will be our first in person meeting after a long time.

So once that has taken place, of course I will report back to you and will tell you more about the workshops that will be held in LA and where the chair and myself as the vice chair will meet with the leaders of the SOs and ACs. So thank you again, Augusto, for giving me this opportunity and I will stay here in case there are any questions or comments. Thank you.

AUGUSTO HO: Thank you very much, León. I will very quickly give the floor now to Carlos Aguirre for his report. And I will kindly asked him to be as brief as possible because we are short of time.

CARLOS AGUIRRE: Thank you, Augusto. I have actually raised my hand to make a question to León, but because of the time restriction, I will skip the question at this point in time, I will make it later, some other way.

So my intention now is to report to you on what ALAC has been engaged in. And it's actually very much related to what León has said. The ALAC CPWG, the consolidated policy working group has a weekly meeting every Wednesday. I will kindly ask the staff to make available to all participants here the link to that meeting, to those meetings.

These are fully open meetings. And that will give you information on what is going on. But nevertheless, very quickly, because of the time we have available, let me tell you that the topics that had been discussed in this Consolidated Policy Working Group are DNS abuse, in the last meeting, we talked about the bulk registration, malicious bulk registration practice that was frequent during the pandemic, and how to mitigate this way of attacking or disrupting or creating complicated situations for end users.

[inaudible] Another point, another area of discussion was the Transfer Policy Review and here there was an analysis made of the blame GDPR has on this, some discussion on the times for the transfer considering the registries' interests. And I think that the region here should work to go deeper into these matters, to promote the Internet end user interests as well.

And this is very personally, what I'm going to say. I believe that oftentimes, individuals who are members of the ALAC committee, because of their seniority, because of their relations, have been

influenced by other positions, basically the GNSO and the Business Constituency. And I believe that there is a strong interest to protect mostly commercial interests of registries and not the interest of the Internet users especially. I think we should work on this in the region and raise the issue.

With relation to DNS abuse, how to enable an easier procedure to submit a complaint for end users how to make this process simpler, how to create a solution, how to see—how to protect the end user who has been attacked.

Another topic discussed in the CPWG is the EPDP on IDNs. Very much related to universal acceptance. There are areas, locations in the globe that use special characters. I remember for instance Myanmar. And another topic is SSAD, the standardized access and disclosure system, which was also a topic discussed in this ALAC group.

The topic that is being discussed now, and we have a deadline here, is the agenda, our schedule for ICANN 74, which is very near and what will be seen in this a new meeting. An additional problem here is that it will be a hybrid meeting, where very few will be able to attend in person and others will participate remotely, how this type of participation will be conducted.

It is true nevertheless that it is seen as a challenge because this is a novelty, this is new for them, for us, the participants. And we are eager to see how this will work for future Internet meetings.

Another topic of discussion that will be the first in ICANN 74 where the At-Large community will take part and it's scheduled for the first date or

the first time, the first session, is something that is also very personal to me. And I think it is also very much related to the GNSO interest.

It's subsequent procedures, what comes in the future. The GNSO is mostly interested in checking what's coming, what's the future of the next round. I really do not know if this is for the end user's interest, benefit. It is definitely among the interests of the Business Constituency and they are pushing it forward very strongly. And that is where we're being involved, because we the ALAC members have to provide advice.

So this is all I can quickly report. Augusto, thank you for this time. And again, sorry to be so open and so quick. And this is because of the time available.

AUGUSTO HO: Thank you. Very quickly, let's give the floor to Sergio Salinas Porto who will give us an update on the progress of the LAC digital program or Forum.

SERGIO SALINAS PORTO: Thank you very much. Good afternoon, good evening. I will be very concise, Augusto, so we can get to the end perhaps on time. We have made progress. We have received the acceptance for the three topics. I think we already have all our speakers. We are trying to get four, but we have already three assured, and this is actually very good, very beneficial to us because the other two topics—these speakers are for universal acceptance.

The other two topics, infrastructure in rural areas and public service, will be completed this week. By the end of this week, I think we have all the speakers, the 12 countries that will be participating. Once that is sent, we will be posting that on the website. We already have the names, the bios, both civil society and government representatives.

I think we are about to have an event for good communication in May. So in a few days, we will have more information on this. And we will certainly make more progress.

As I said last week, I will be submitting a written report to the region as I've done before. And I take this opportunity to say my friend Alejandro Pisanty that tomorrow by e-mail and later by phone, I will discuss this intervention. That is all. Thank you very much.

AUGUSTO HO: Thank you, Sergio. Thank you for this update on what is going on with LAC Digital. Now I'm going to ask Claire to present on the 2022 elections. Claire, you have the floor.

CLAIRE CRAIG: Hello. The 2022 elections, there are two positions that are available at this time for this year. I think you should be seeing it on the screen right now. Those positions are the ALAC representative and that is for region D, which is Argentina, Brazil, Paraguay and Uruguay, and then the NomCom position, which is region [inaudible] and that is Central America and Mexico, Belize, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Mexico and Panama.

Today, the 18th of April, there is the announcement of the call for nominations and the nominee statement. Between the 18th and the 29th of April, we have the nomination period. And that's 10 working days, the 26th of May is the deadline for nomination acceptance, the 9th of May to the 12th of May calls with candidates if desired by the RALOs.

Then the 13th to the 20th of May elections, if required, will be begin no later than one week after the deadline for the nomination acceptance and no later than two weeks after that deadline. Finally, at the 2022 AGM, which is ICANN 75, the newly elected ALAC members and RALO leaders will be seated at the end of the 2022 AGM following the close of the Board meeting on September 22nd 2022.

Now this information is also available on the Wiki site. I know I had to go very quickly, but please review it there and make your nominations. Remember that the particular territories that are up for elections at this time are region D for the ALAC and region [inaudible] which is Central America and Mexico for the NomCom. Thank you very much.

AUGUSTO HO: Thank you very much, Claire. So we're past our time. We will have to close today's meeting with some areas still pending to be discussed next meeting. And finally, kindly ask you to fill in the survey. We have a couple of minutes for Vanda to use these two additional minutes. Vanda, you have the floor.

VANDA SCARTEZINI: Thank you. It was just a request to report to you that everything went very well with the face-to-face meeting held in Washington, United States for the entire NomCom.

So we were like 14 people, everything went very well. We were tested on a daily basis every day at 7:00 AM in the morning before entering the meeting room. So we were all healthy and did all without problems. So I wanted to share with you that everything was very well organized, of course, with the difficulties of transportation and the rest, but without any serious problems.

Everything went very, very well with the staff in Los Angeles and the rest of the world. They provided their support remotely, as well as three colleagues, other NomCom members that were not able to get their visas on time for the meeting. So they attended remotely over the phone.

It was very good, very well organized. So we had a very nice conversation, we took some pictures as well, outside, outdoors. Everything went very well. I just wanted to share with you that this experience was useful and a success. So we are happy to see how it all went. Thank you so much.

AUGUSTO HO: Thank you, Vanda. And now Silvia, unless we have anything too urgent, we can close.

SILVIA VIVANCO: Yes, this is all. And please, all of you fill in the survey that will be shown as soon as the Zoom is closed. And thank you for attending this session.

AUGUSTO HO: Thank you very much, and good evening.

[END OF TRANSCRIPTION]