ICANN68 | Virtual Policy Forum – Plenary Session: The DNS and the Internet of Things: Opportunities, Risks, and Challenges
Tuesday, June 23, 2020 – 13:00 to 14:30 MYT

RIA OTANES: Hello, and welcome to the plenary session on the DNS and the Internet of Things: Opportunities, Risks, and Challenges. My name is Ria Otanes, and I am the remote participation manager for this session.

Please note that this session is being recorded and follows the ICANN expected standards of behavior. During this session, questions or comments will only be read allowed if submitted in English within the Q&A pod. This feature can be accessed from the Zoom toolbar. I'll read questions and comments allowed during the time set by the chair or moderator of the session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, you'll be given permission to unmute your microphone. Kindly unmute your microphone at this time and take the floor. State your name for the record and the language you will speak if speaking a language other than English. This session includes real-time transcription and interpretation. To view the real-time transcription, click on the closed caption button in the Zoom toolbar.

To assist our interpreters, kindly speak clearly and at a reasonable pace. To hear the interpretation, you will need to download the interpretation application. More information can be found in the session details on the event schedule, and instructions are in chat.

Lastly, I would like to remind you to use the drop-down menu in the chat pod to switch from respond to all panelists, to respond to panelists and attendees if you would like everyone in the room to read our chat comments.

With that, I will hand the floor over to Alejandra Reynoso. Alejandra, please go ahead.

ALEJANDRA REYNOSO: Thank you very much, Ria.

Warm greetings, everyone. My name is Alejandra Reynoso. I work for .grant Thornton, the ccTLD of Guatemala, and I am honored to chair this plenary.

The Internet of Things promises to make our lives easier and our societies safer, smarter, and more sustainable through tens of billions of connected devices that passively and autonomously sense and act upon our physical environment. While this makes the IoT vastly different from traditional interactive Internet applications like email and web browsing, many IoT devices will use the Domain Name System to locate the remote services they need.

The Security and Stability Advisory Committee, SSAC, recently published the document SAC105, a report that discusses the opportunities, risks, and challenges of the interaction between the

DNS and the IoT. Today's plenary will give further substance to the dialogue that this document aims to trigger, specifically by enabling community members from all constituencies to discuss the topic with subject-matter experts as well as with each other.

This plenary is a follow-up from the ccNSO session on SAC105 at the Montreal meeting which had a particular focus on ccTLDs.

The goals of this plenary are to better understand how the Internet of Things differs from traditional interactive Internet applications and how it uses the DNS; to better understand how DNS and IoT players think of the interaction between their two ecosystems in terms of opportunities, risks, and challenges; and to advance the thinking on the role that the ICANN community could potentially play in this space.

Next slide, please.

This will be today's agenda. First, there will be a brief overview of the document SAC105. Then we will have an experts panel to share their perspectives on the topic. Afterwards there will be a peer review where the reviewers will provide feedback on the presentations from the experts. And we will end with questions and answers from the audience.

Next slide, please.

Let me briefly introduce you to Cristian Hesselman who will give us an overview of SAC105.

Cristian is the director of SIDN Labs, which is the research team of SIDN, the operator of .NL Country Code Top Level Domain of the Netherlands. Its goal is to advance the operational security and resilience of end-to-end Internet communications through empirical measurement-based research and prototyping and evaluating new Internet systems and tools.

Cristian is also a member of the SSAC and led SSAC work party that produced SAC105, the DNS and Internet of Things, opportunities, risks, and challenges.

He is also a part-time associate professor at the University of Twente, The Netherlands, and chairs the Board of Directors at NLNetLabs.

Cristian, the floor is yours.

CRISTIAN HESSELMAN: Okay. Thank you very much, Alejandra.

So it is my honor today to give you a short overview of SAC105, which is the report that the SSAC released in June of 2019. And as Alejandra already summarized, this document is on the interplay between the IoT, the Internet of Things, and the DNS with a particular focus on triggering and facilitating discussion in the ICANN community.

So this report will also be appearing as a peer-reviewed paper in magazine called IEEE Internet Computing somewhere later this year.

Next slide, please.

So the Internet of Things. What we used as a definition in our report is the definition of the IoT that ISOC gave back in 2015 which is an application that -- well, what it says there, extends network connectivity and computing capabilities to objects, devices, sensors, and items not ordinarily considered to be computers. So basically connecting everything to the net that you weren't thinking of connecting before.

The differences with traditional, you know, interactive applications like email and web browsing, some of them are the following. So IoT continually senses and interacts with physical space. That's an important difference. And it also interprets the information that it receives from various sensors to actually act upon that space. This usually happens without user awareness, so think about tiny sensors embedded in, you know, walls and other kinds of objects that you interact with without really knowing it. So that's what the ISOC people call passive interaction as opposed to interactive interaction that you would have with web browsers and email clients, for example. So there will be a vast amount of these IoT devices. At least that's the projection of many market analysts. So people are mentioning numbers of 20 to 30 billion of these devices, and they're, you know, basically operating in the background of our daily lives. So we don't actually see them. We interact with them without being aware of them.

Also what's a difference is IoT devices are typically much more heterogeneous than what we're used to in terms of laptops and mobile phones. So we're talking about different types of operating systems. We're talking about different hardware architectures, and we're also talking about different types of network connections. So it's not just Wi-Fi. It's also ZigBee, it's also other types of wireless networks.

Okay. And also, finally, the IoT differs in that the IoT devices have much longer lifetime, perhaps because they're embedded in physical structures, for instance, and they're also characterized by their unattended operation. So there's no network manager or anything like that that really looks after these devices. They're just sitting there and doing their thing and connecting to the net without you guys knowing it.

So IoT is considered to be the next, you know, big thing for a while now. Actually, this stuff has been going on since the 1990s, I think, and it used to be called pervasive computing or something like that. So there have been different names for roughly the same concept. But anyway, now we're getting at a stage where it's possible to really deploy these kinds of devices, sensors, and actuators, and as a result, people think that -- there's a strong belief that IoT will promise a safer, smarter and more sustainable society. For example, in the area of intelligent transport systems, so intelligently routing traffic through an urban area, for example, based on all kinds of sensors, or smart energy grids or perhaps smart homes and smart cities. I think the latter is the most appealing example because that's what we all know because of all the stuff we have in our houses at this day and age.

Okay. So there's a lot of, you know, promise in the IoT, but there's one major issue, which is IoT security, and I'll be talking about that in a minute.

Next slide, please.

Thank you.

So this is an example of the -- This is the model that we're using in the -- in SSAC to think about the Internet of Things. So what you're seeing here is kind of a busy picture of physical spaces on the left, so let's take the top part. So those, what you're seeing on the top left are people in their homes, and they interact with what we call an IoT deployment. That's basically the shaded area like you are seeing in the middle of the screen. And an IoT deployment consists of three different things. One is IoT devices. Two is network connectivity. And three is back-end services, right?

So there's an example here with a small watch and a smart door lock where when somebody approaches the door and people get close to the door of their house and they perhaps also have some sort of smart doorknob, all this information about the proximity gets collected by -- from a smartwatch that folks are wearing in combination with, you know, fingerprinting done by the smart doorknob, and that information is being sent over the Internet to a service somewhere that's a remote service, and based on that service the decision is being made, okay, let's open the door lock or not. That so that will be driven by user policy, obviously.

So what you're seeing is that in this very simple example, there is information being sensed by the top device, D1, by the smartwatch, for example. That information is being shared across the Internet to a service and then sent back again to the door lock to lock it or unlock it.

So what you're seeing is sensing and acting upon the physical -- sensing of and acting upon the physical environment of the user, and that takes place transparent -- without users being aware of it, right?

So users only see the devices, so they see their smart watches and they see their smart doorknob, for example, but they don't see a whole machinery that's sitting behind that.

And one of the pieces in that machinery is the DNS, because what we know from, you know, previous research is that these devices, they have -- they interact with services on the Internet to provide their functions, right? So -- and that's different from traditional web browsing where you interact with a web browser to pick up some information from the web or to use a service. This -- in this constellation, devices are using services to perform their function, right?

So for example, in this specific case, the service could be analyzing the sensor information coming from the user and then make a decision whether to open the door lock or not. Okay?

So in these interactions, the DNS plays an important role, but I'm not going to discuss the details because Eliot is going to be speaking about that more after this presentation.

Okay. I think that's the most important bit for now, so please continue to the next slide.

Okay. So this report is called DNS and the IoT opportunities, risks and challenges. So I'm having a slide on each of these three: one for the opportunities, one for the risks, and one for the challenges. And opportunities is something that we usually don't really talk about in the DNS because -- in SSAC because we are mostly focused on threats and risks, as we should, but in this case we thought there was need -- there was an opportunity for the DNS because it's a global -- you know, it's a global trust infrastructure, you could say, that would be able to increase the privacy, safety, and transparency of the Internet of Things. So we really believe that the DNS can provide an added value here.

So I listed three here. More details are in SAC105. So the first one is that we think that the DNS can reduce the risk of users being profiled, and that's because these devices that we just talked about, they interact with the DNS. So the DNS queries, if there is an observer between the path of the IoT device and the remote service that it uses, it can see, based on the DNS interactions, what a person in their house, for example, what kind of devices they are using or what -- perhaps even if they are using a device, because that creates more interactions with the DNS.

And another possibility is that if you know which IoT devices are being used by looking at the domain names, you can even -- as an attacker, you could even try to come up -- try to figure out what the IoT device is that's generating these queries, right? So there's more research that shows that many IoT devices use a small set of domain names that they query, so to find that remote service that we just talked about in a previous slide. And sometimes these DNS queries or the domain names that they use, they also reveal information about the type of device that's generating them, okay? So that's the thinking behind this part of the reduced risk for user profiling. And you can achieve that by obviously encrypting the DNS requests that these IoT devices generate. So you can do that, for example, through the much-debated DoH and/or DoT.

Another opportunity that we foresee is that to mitigate a risk where IoT devices are being redirected to another remote service. So, for example, we've seen -- on the Internet, we've seen a concept called route hijacks, for example. And they result in traffic being sent to a malicious network. And that's something which could have severe effects in the IoT because IoT devices would no longer connect to their -- the services that they're supposed to connect to but perhaps connect to a malicious service. And the risk there is that folks are sharing their data with -- intimate data with remote services or that means remote services could even act upon their physical environment, right? So that's a risk.

We think that the DNS can help here because obviously we have the DNS -- DNSSEC, right? So it can validate the integrity of the messages coming out of the DNS. And if a routing hijack occurs, as an example, then DNSSEC clients will be able to detect that because they can --

they notice that because the signature on the DNSSEC messages don't validate.

And another opportunity here that we see is that -- that it's an opportunity for registrars to provide multifactor authentication. So that's what MFA stands for.

For example, they could protect domain names that are being used by IoT devices more heavily by using multiple factors, maybe even fingerprint recognition or something like that. Okay? So those are the two opportunities that we see to reduce the risk of IoT devices being redirected through a malicious service.

And then, finally, we see an opportunity for providing more insight into the services and resolvers that IoT devices use. So most of the time, people interact with IoT devices but they don't really know what kind of information they're sharing with what services on the Internet. And by, let's say, making the DNS queries that the devices of users generate, making them visible to end users will help them give more insight to those interactions, okay?

So in the previous example, you would see that -- you would be able to see that your watch shares information with a remote service on the Internet, for example. Okay?

Next slide, please.

So this is the flip side, the risks. So maybe I should only talk about the -- I will try to shorten this one a little bit. So the biggest risk that we see is that the IoT results in large DDOS attacks on the DNS, right? So when we've seen this before, of course, the infamous example is the DDOS attacks that took place on the 2016 on the DNS operator Dyn. But we have also seen other IoT botnets developing on the Internet, and they can grow in size quite quickly. Potentially they could also start using open resolvers that would reflect DDOS traffic off of them toward their target and that would even create an even higher amount of influx-ed traffic for those people.

And the other risk is what we call DNS unfriendly programming, which is using the DNS in a kind of naive way, that -- so, for example, we had -- a couple years ago there was an example where a iPhone app generated random DNS queries which caused resolvers to blow up their caches because they couldn't cache anything and they ran out of mirroring.

Next slide, please.

So we've seen -- we discussed the model of the IoT that we have developed at SSAC. We discussed opportunities, and we discussed risks. So the next question is: What should we do to seize those challenges and address the risks?

So we came up with a few challenges for the DNS and IoT industries that we wrote down here. So this actually goes to a little bit further than the scope of SSAC because we also think there's a role for the IoT community in here.

So the first one would be to develop a security library for these IoT devices that would provide these functions that we just talked about on the opportunities slide. So that would be DNSSEC validation, for example, and DoH/DoT support, and also functions that would make DNS queries visible to end users in an attractive and intuitive way.

Then we think there's a challenge for training. So training IoT experts to understand what the DNS is about and what its security functions are and what you need to do to use them and the other way around for DNS experts to basically understand how the IoT works and perhaps also that the IoT will change the way that domains are being used and perhaps this requires different types of functions for IoT -- for domain name registrations and security.

The last few are perhaps a bit more challenging, the more challenging challenges. So the first one would be to collaborate with a group of DNS operators to share what we call DDOS fingerprints. So those would be summaries of DDOS attacks that took place on these DNS operators. They would then share that information with each other to be better prepared.

It could also be that these DNS operators even try and share DNS-mitigation capacity. So, like, scrubbing facilities, for example. And we foresee a role for systems in edges of the network to protect the edges against DDOS attacks and also against intrusions. Device intrusions, that is.

And, finally, dreaming a little bit, it would be very nice, we think, to have a system that is able to measure the evolution of the IoT and to see how it grows and how it uses the DNS.

And those were my slides, Alejandra.

ALEJANDRA REYNOSO: Thank you very much, Cristian.

We will now continue with our experts panel who will share their perspectives on the matter in the following order. First, Eliot, second Lise, and third Cristian.

Let me first introduce you to Eliot Lear and Lise Fuhr. Eliot Lear works as a principal engineer of Cisco Systems in the area of IoT security, focusing on how the device and the network communicate with one another. A veteran of the Internet community, Eliot has been involved with the IETF community since 1998, has written a number of RFCs, served on the Internet Architecture Board, and was a leader of the IETF contribution to the restructuring of ICANN during the IANA transition. He has also served in leadership roles in the ITU. Eliot resides in Switzerland.

Lise Fuhr is the Director-General of the European Telecommunications Network Operators Association, ETNO, since January 2016. At ETNO, she leads and oversees all the activities as she is the main external representative of the Association.

On behalf of the Association, she's also a board and an administrative committee member in the European cybersecurity organization. Lise has also been reappointed to The Internet Society Public Interest Registry Board of Directors for a three-year term as of May 2019.

Lise has 20-plus years of experience in telcom's industry. She started her career at the Danish Ministry of Science, Technology and Innovation where she wrote and implemented regulation for the telecommunication markets. After that, she worked for the telecoms, operator, telenetworks where she led various teams dealing with issues as they process interconnection devices, mobile devices -- sorry, mobile services and industry cooperation.

Eliot, the floor is yours.

ELIOT LEAR: Thank you very much, Alejandra.

So next slide, please.

I'd like to tell you a story about an oven. This is an oven. It is Internet-enabled. It is IoT-enabled. And my cousin bought one of these, installed it, and some time later it paged her at 5:30 in the morning to let her know that it needed to be cleaned. Now, personally I view this as a denial of service. But this is the way it was designed to work.

What my cousin didn't know is in order for all of that to work, there were a lot of components available in that device. Not only did the oven have a heating element and a thermostat, the appropriate insulation, and all the other things ovens have, but it also has a transceiver, a CPU, some memory and some soft switches and a display.

That represents a threat. That is to say anything with those components can be attacked. And so what could one do in such an attack? Well, if one was successful, one could perhaps burn my duck or, in worst cases, one could create a coordinated attack in which all ovens turn on at an inconvenient time. Say, in a region that doesn't have excess power due to hot weather and air conditioning. And all the ovens going at once does create a brownout.

Moreover, much of the software stack in that oven is used by other devices, maybe air conditioners, maybe stoves, maybe radios, maybe doorbells. And so a lot of devices could be enabled all at once to generate a huge power demand. So some protection for that oven is needed.

Next slide, please.

Next slide, please.

In order for that oven to work -- it didn't just directly page me. Here we have a picture of the Internet, a very great picture of the Internet created by KC and her team some time ago.

Next slide, please.

The oven actually spoke to devices in the cloud in order to do that. And it did this just as the doorbell does. So this is a common usage pattern.

Back up one, please. Thank you.

And it was the cloud devices that actually communicated to her iPhone. And this is a common pattern.

In order for these devices to communicate with the cloud, they need to use the Domain Name System. They have a cloud-based endpoint. It's something like cloud.example.com. And that is how they communicate.

Now, in order for them to communicate at all upstream on the Internet, the information has to be routed by the nearest router.

For the oven in question, and for that doorbell, we're talking about WiFi. But there are many other means to do that. But a lot of this is, indeed, communicated through the home, through the home router.

Next slide, please.

So how does this work? You receive, for instance, a query interest the oven -- next slide, please -- where queries say ovencloud.example.com, and an IP address is returned. And an IP address is something that comes from a specific address. Now, keep in mind what Cristian said. There are some 20 billion of these devices that are out there. We have a great many devices on the Internet, but the oven only needs to talk to its cloud end point, maybe a handle of end points, maybe some devices in the home, but it doesn't need to talk to everything.

And so if that -- that home router can provide a control point, and that control point limits the threat surface of that oven. And so what that means is that even if there is a bug or vulnerability in the oven, the control point can protect it from broad-scale attack. Does that mean that the oven manufacturer shouldn't provide software updates when it finds bugs? Obviously not. Still -- there is still a threat surface even with some of these network protections, but the network helps to reduce that threat.

Next slide, please.

So here is the communication that goes to the device, the cloud end point that has been resolved by DNS. In order for the control point to function, it needs to receive the query and response from the oven. So this means that if the DNS query is encrypted and the control point is not aware of it, then it cannot provide protection and it cannot reduce the threat surface.

Next slide, please. And of course this repeats with doorbells and quite a number of other consumer devices.

In the industrial world, things look a little different. Today I'm focusing primarily on what you would see in consumer devices. We see various different cloud end points that are used by various different devices.

Next slide, please.

So what does all of this mean? It means that we need to -- It's okay to encrypt. There's good reason to encrypt DNS queries, and Cristian mentioned a lot of those. However, if the control point -- if your network router that is intended to reduce the threat surface cannot itself have access to the query, if it's not an authorized party in some way to see the communications in terms of the -- both the query and the response, then that router cannot provide the necessary protection. So there is this binding between the DNS and the router that enables this protection. And this work has been standardized at the IETF as one means to provide that protection.

So we're not saying don't encrypt. Quite the opposite. We're saying do encrypt. But make sure that when you do encrypt, it is to a component that is authorized to provide some of (indiscernible).

I think that's my last slide.

Alejandra?

ALEJANDRA REYNOSO: Thank you, Eliot.

Now we will have Lise.

LISE FUHR: Thank you. And hello, everyone. I'll bring another perspective, since I'm coming from the telco side, the ISP.

Next slide, please.

So if -- my presentation will be around why is it interesting to talk about 5G and Internet of Things. I'll talk a bit about what is 5G bringing of new opportunities, but also I would like to address some concerns that have been raised around 5G and DNS, and also saying where do we see the world goes from here in relation to 5G and Internet of Things and DNS.

Next slide, please.

So if we are to see -- talk about Internet of Things, why is this interesting in relation to 5G? It's because we actually see, as telcos, that 5G, which is a mix of both fixed networks and mobile networks, it's not a new just a 4G technology. It's a much more converged technology. So we see that would actually enable and be an important component in the growth of IoT.

So you see the numbers here, which is only on mobile IoT and might even be a very low number, saying that in 2018, we saw 140 million mobile connect -- IoT connections, and we expect nearly 740 million by 2026.

What will be the new thing that will be interesting in 5G? Is that will be the narrow banned IoT, and also of course there will be some machine -- some MTC enhancements that are the next -- that will be a development of what's there in 4G.

So when we look at 5G, it is -- it will be a number of services already building on what's there on 2 and 3 and 4G, which is already now supporting IoT. But the new IoT will be much more IP infrastructure, and then also much more DNS infrastructure.

So right now, what we see is not what we call IoT, which is on IP as much but more on other services. And we expect that we will have another use of 5G IoT than the use we have today. And we think it will be a better and more secure use.

So if we look at it as it says on this slide, IoT and the 5G IoT doesn't grow in a vacuum. It's actually building on a broader service portfolio. And DNS and IP in general will be a federator here.

Next slide, please.

And if we look at the inheritance of 5G mobile and DNS, 5G is not going to be a 5G standalone from day one. Right now, what we see is that there are a lot of 5G networks that are building on 4G infrastructure. So what we see is 4G with 5G equipment, but it's not a fully fledged 5G network.

And there, the use of DNS and domain names in these mobile core systems, they're not prevalent, but we do use a lot of DNS, but it's limited so far.

And we do see, of course, exceptions for routing relying on DNS where VoLTE is one of the cases. But what is it that we use domain name for in the mobile system? We see the interdomain name is limited right now, and they are deriving from legacy IDs, and mobile Internet access is nonspecific. Well, that's to mobile.

So there is nothing new in 4G to 5G use in relation to DNS, but we use it the same way in 5G as we did in 4G. Next slide next slide, please.

So why is it 5G interesting and why is it more interesting than 4G? That's because, as I said, it's a much more converged network. It is a virtualized network that will be using a lot more software and not as hardware dependent as 4G. It will be a more flexible network. And as we say, it's intended to be IP native. And while it's tricky to actually manage and operate with IPv6 addresses because they are so very long, we still see a strong use of DNS for this because of IPv6 structure.

We also see that our interdomain will be IP native, and we will gradually move to IP into domain names in the way we manage the network.

So it is -- In Europe, we still largely operate our interconnect on circuit switch based, but we think that with 5G we will have much more IP interconnect. So that's the way the evolution goes on how the 5G network will be operated.

Next slide, please.

So if we are to look at how the use of domain name will materialize, essentially it is transparent for users in the meaning that it's invisible for the users how we use the DNS. So the way we work with our networks is mostly for technical purposes, and it will be embedded in the device, so the use is not supposed to tie the domain name. So the name is not a very important part of this, but of course the DNS technology is.

And, again, on IoT, how it's being implemented is -- is really the key here, because it's how we implement it that actually defines how the setup is. So while we see that 5G is not -- we don't believe 5G will be a significant source of new second-level registrations, we actually think that this will be defined by much more subdomains. So we don't expect a spike in how we use domain names because it is defined to be more subdomain used. And again, much of this is not really to be resolved on the Internet but will be resolved as an interdomain or intradomain name.

Next slide, please.

So why do we think that 5G is beneficial for IoT and Internet of -- and DNS? First and foremost, we think that at the core network level, we will have, as I said, a lot more software and that will enable and make it much more flexible and easier to work with machine-type communication in narrow band. We are able to define the networks in a much easier way with 5G. And on the security side, network slicing will be extremely important for us. Network slicing will be part of the network where we can define it for this specific type of use. For example, automated cars, which is a huge IoT, will need very low latency bands. And so there it's important that we have one kind of services for automated cars.

Also, the use of AI we think will actually open standards our networks, both in the way that makes them better but also enable us to find if there are any threats or issues with the networks. We think AI will enable us to work much faster and find the issues in a better way.

So back to the challenges, and next slide, please.

If we look at what we see as the challenges and how we can mitigate them, we think network slicing is extremely good. There have been concerns that this will create a fragmentation of the Internet. We're not seeing this as any issues at all. We think this will be like VPNs, and it's still -- it's much more targeted services for the end users and will not create any fragmentation of the Internet.

If we look at domain names and collision avoidance, we're using public domains and we are not seeing this as an issue. If there is any domain that we use for internal routing, it will be a public domain and not create any collisions here.

On the DNSSEC side, which is an important thing, it will be an opportunity. It's not a standard -- it's not a mandatory standard at the moment on 5G. We have not seen things that would create a need for having DNSSEC as a standard in the 5G network, but it is to be used.

And then, again, on denial of services and DDOS attack and botnet, in the 5G network, we can, of course, handle this. But there is an encryption trend. And if you are to monitor these attacks, we need to be able to see the traffic.

So on the denial of services, if we are to be an active part in this defense, we need to be able to see the traffic.

Next slide, please.

So where do we go from here? There is still many open questions on the standardization of 5G. We're just in the making of the 5G networks. And, as I said, we haven't seen many stand-alone 5G networks so far. So what we're building on now is 4G with 5G components.

The infrastructure is expensive. So as I see it, 5G is not a fully-fledged stand-alone. 5G is not around the corner because the business case of (indiscernible) these networks are extremely expensive.

One last thing is we actually saw the COVID crisis, which was a terrible crisis for all of us, but we saw all over the world that there was a strong focus on the need for digitization. We saw a stronger focus on security.

So from that perspective, we saw that there was a growing awareness that the infrastructure is important, that the security is important, and also that we saw an enhanced use of our networks. So we think the future will bring less traveling. We're here today. A very good example that none of us has traveled to an ICANN meeting, instead we're doing this remotely.

And in relation to IoT, we also think that this will, of course, also as an outcome of this crisis be creating more remote monitoring and more IoTs.

That was my part. Thank you.

ALEJANDRA REYNOSO: Thank you very much, Lise.

Now we will have Cristian.

CRISTIAN HESSELMAN: Yes. Thank you, Alejandra.

So I'm switching hats basically. I previously -- I was previously wearing my SSAC hat. Now I'm turning to my .NL hat, which is the -- so next slide, please.

So .NL is the registry for The Netherlands. We are a small country in Europe. We can be begin, though, because last week we reached the 6 million domain name mark. So that was a really cool and cause for celebration online.

But one of the important things that we do is that we -- one of our important tasks is that we aim to improve the security and resilience of the Internet, as you can see on the slide. And that's why a couple of years ago we decided to start working on IoT specifically to address some of the challenges that I spoke about earlier when I discussed the opportunities, risks, and challenges part of this presentation.

And the reason that we started doing that is on the next slide. It's basically the Dyn attack that occurred in 2016, so a DNS operator was attacked by a botnet that sent a lot of traffic. The botnet was hundreds of thousands of infected IoT devices, and it sends a lot of traffic at the same time toward its particular target. And as a result, it caused outages of popular services, services like Twitter, Spotify, and whatever else.

So when we saw that, we thought, We're a DNS operator. We're a critical infrastructure for the Netherlands and also for the Internet at-large, so we want to do something about that. That's when we started developing the SPIN prototype. So SPIN is an acronym for security and privacy in in-home networks.

And the purpose of the system is to basically monitor -- so you would place a device in your home network or you would enhance your home gateway, as Eliot talked about, with additional security functionality. And this functionality would then monitor your local network for any DDOS traffic, for example, so for signs that one of your IoT devices at home would have been infected by a botnet, for example, and would be participating in one of these large DDOS attacks.

What we would then try to do is try to temporarily disconnect that device from the Internet so as to protect the Internet infrastructure from these DDOS attacks. So it's kind of a reverse firewall, if you will.

And so this is an example of something that we developed at SIDN. This system is currently in a prototype stage, although last year we kind of invested in this software to bring it to a production level because what we wanted is to help ISPs and to help consumer equipment manufacturers to also use these types of functions on their devices. But this turned out to be much more difficult than we thought because it's a different ecosystem than the DNS ecosystem that we're used to.

And also there's -- it's a different business ecosystem, so to speak. So, for example, ISPs, at least the one we spoke to, they are struggling with how far they should go in helping their customers with solving security problems of their IoT devices that they did not certify. So they are kind of reluctant because these kinds of additional services can cause a load on their support, for example, which introduces additional cost. So that's kind of one of the factors that makes the deployment of these kinds of system difficult.

And another factor is the equipment manufacturers, they basically -- they basically add these functions if their customers, so ISPs, ask for it. So there's also a chicken-and-egg problem there.

We do know this is an important problem, though, because if you look at -- at least in Europe, if you look at the Dutch National Telecommunications Regulator, they have a specific program on IoT security. And there's also initiatives in the European setting where folks are trying -- where different telecom regulators from within Europe are trying to extend the radio equipment directive which is our regulation for any device that has -- that does radio transmissions to extend those specifications with baseline IoT security requirements. So that indicates that this is an important problem from a public perspective, so to speak. But there is more traction to be gained in the industry, in particular in the ISP world. The connectivity world, I should say.

Next slide, please.

The software you just saw was open source. You didn't see the software. You saw the picture. The URL, if you want to get it, is down there.

Another example of the same prototype that we developed is increased IoT transparency. So you may remember that previously I spoke about the opportunity for the DNS to visualize DNS queries for users in an intuitive, easy-to-use way. And we developed a prototype to illustrate that. That's what you're seeing on this screen here.

So, basically, the gray circles, they are devices in the network. The one at the top, I think, is a phone because it has many devices that it connects to.

And the blue and the green shapes, those are basically remote services that these devices connect to. So this is a screen shot.

And the actual application is very dynamic. You see the -- actually you see the interactions with the remote services popping up as they occur. So this is based on the analysis of the DNS queries.

And I should add that SPIN is a privacy-friendly solution because it keeps all the measurements and the analysis within the home network. So it doesn't share it with cloud services or stuff like that.

Okay. So these were two examples of, you know, systems with which we are trying to address the challenges that we spoke about in the SSAC report.

Then I have one more example, which is on the next slide.

And this last example is really about what ISOC a couple of years ago, what they called collaborative security. So multiple organizations working together to secure the Internet, which is actually essential to the Internet because the Internet is one big collaboration. So if you want to secure it, you will need to do that together.

And one of the examples that we're involved in is what you're seeing here. It's called a DDOS clearinghouse. And its purpose -- it's a centralized system currently that enables folks to share summaries of the DDOS attacks that they handled on their systems. So they get inbound traffic. They generate a fingerprint of that, and they share the fingerprint with other operators within that group so that these other operators know that there's -- this kind of attack has occurred and they can prepare their infrastructure in case the attack comes their way next.

So it's really being about proactive. For the victim, it's too late. It's still reactive. For the other ones in the group, it's proactive because they have more information about the DDOS attacks and that would occur at other service providers.

So this is basically an information layer that you would add on top of your existing DDOS mitigation infrastructure. It's not replacing it. It's an additional system -- distributed system that you add on top.

And this is something we're currently piloting in the Netherlands. So there's a cipher, which I forgot to mention here, it's called nomoreddos.org. So go check it out. There's a blog with additional information there.

We are currently exploring -- we are currently setting up a pilot in the Netherlands which in itself is part of a larger European project called CONCORDIA, which is on cybersecurity in general. But there is -- one-quarter of that project is really about these DDOS clearinghouses.

And we think that -- we currently organized the DDOS clearinghouse in a national way. So this means that the members are organizations from the Netherlands, like governments, ISPs, Internet exchanges, the registry, and many more organizations. Banks, for example.

It's also possible to organize it in a different way. You can also imagine a DDOS clearinghouse for the DNS industry, for example, where DNS operators at the registry and maybe at the registrar level would collaborate to share information about DDOS attacks.

These are basically three examples that I wanted to give from .NL perspective that we hope help solving those -- help addressing the risks and seizing the opportunities that we spoke about in the SSAC report.

Thank you.

ALEJANDRA REYNOSO: Thank you very much, Cristian.

Next slide, please.

It is time now for the peer review. Please meet our reviewers. We have Philippe Fouquart. He's a representative of the Internet Service Providers and Connectivity Providers constituency, ISPCP. Philippe is a senior expert in naming, numbering, and addressing at Orange Labs Networks. Since 2001, he has been in charge of NN&A activities within Orange Labs to design Orange's networks' architectures and provide technical support in this area to business units within the group worldwide.

Rafik Dammak is a computer engineer working and living in Japan after finishing his masters in applied computer science at the University of Tokyo. He has been involved within civil society and Internet governance issues since 2007, attend several Internet Governance Forums, and other Internet-related conferences either as a speaker or workshop organizer.

His main area of focus is in ICANN policy-making processes where he has been involved in different roles within Noncommercial Users Constituency, NCUC, and Noncommercial Stakeholder Group, NCSG, and on developing awareness on Internet governance issues in the MENA region.

Kimberly KC Klaffy is director of the Center of Applied Internet Data Analysis at the University of California San Diego. In 2017, she was awarded the Jonathan B. Postel Service Award and inducted into the Internet Hall of Fame in 2019. She's also an adjunct professor in the computer science and engineering department at UC San Diego. Her research interests span Internet topology, routing, security, economics, future Internet architectures and policy. She has served on ICANN's SSAC since 2003 and holds a Ph.D. in computer science from UC San Diego.

Peer reviewers, the floor is yours.

We can start with Philippe.

PHILIPPE FOUQUART: Thank you, Alejandra. Can you hear me?

ALEJANDRA REYNOSO: Yes, perfectly.

PHILIPPE FOUQUART: Thank you, and thanks to all our panelists. So a few take-aways and possibly a comment for mine. Eliot introduced use cases where IoT is essentially a device to serve a framework as opposed to being device to device. I understand there's an argument for having an IoT-owned gateway for the local network not completely blind to outgoing and incoming DNS request, the reason being that ingress filtering can be used to reduce a number of security threats.

Lise, you distinguished between the two dimensions that you see in 5G mobile networks, one being IoT on the mobile Internet and IoT application and services as provided by an operator. And you said that 5G and slicing was not a threat to the one Internet, one DNS (indiscernible). And there are architectures where DNS architectures are used already in mobile network, and those are different from the DNS that we know on the Internet. So there's nothing new there.

And finally, Cristian discussed the concept pilot of an IoT DNS gateway through the SIDN's SPIN to monitor outgoing DNS traffic; in particular, with a view to combating DNS Denial of Service attacks.

So those are my take-aways from the talks.

One comment or question from me on the challenges. The IoT being a complex ecosystem of players which may not be involved in this organization or those that are in charge of defining the standards, for instance, there's always the very general question of how you promote or enforce good practice of project goals in general and DNS in particular. And how you reach out to -- with that community of players.

So maybe to our panelists or as food for thought, I'd be interested in learning more about how -- where you stand in the ecosystem, whether you're an operator, a registry, or a vendor. How we can reach out or you can reach out to that community of device makers to promote those good practices.

Thank you. Back to you, Alejandra.

ALEJANDRA REYNOSO: Thank you, Philippe.

Regarding your questions, I think our experts will think of them a little bit more, and if we could pass through the other reviewers and then in the end come back to your questions, that will be awesome.

Can we hear from Rafik now.

RAFIK DAMMAK: Okay. Thanks, Alejandra, and thanks to the panelists for the presentations.

So I also have a few take-aways and try to kind of understand here maybe the scope.

So I think one of the important questions is it seems quite outside the remit of ICANN and SSAC, but because what the DNS has technology here or ecosystem can provide to IoT that's an interesting topic for us, but maybe what I could notice is we talked about how maybe the different player, the IoT player, the ecosystem and the different actors, maybe they -- how they need to do in terms to improve the security and safety, it was not clear for me what can be the role of the user. And maybe it's not that straightforward, but what we are expecting from the user? What kind of awareness we need on their side as consumer of those different technology? Sometimes even they are impacted by those technology, I mean, when we are talking about the IoT and all those smart home devices where they are not a direct consumer.

When -- I think Cristian talked about how we need to help in term of using, maybe that's my wording here, wisely the DNS and the best practices. I am wondering, from the own experience in ICANN, like when we introduced the new gTLD and IDNs and we had that experience about universal acceptance, how that can be useful or appropriate in term of a learnant (phonetic) -- a listen learnant or a approach, too, that can be leveraged for helping to spread or to use more about better usage or the best practice regarding the DNS and the IoT context.

So I'm wondering if maybe Cristian, based on his own experience and also with what he -- he worked on the .NL, he can develop on that and see if there is any common areas and what we can learn from that experience.

Just maybe another point. It's -- I think it was good to hear more about the 5G and how it's useful for -- in IoT context. And maybe to learn how the DNS is used on that -- in that area. But maybe if Lise can develop more into the extent if there is any policy area that we need to be aware about with regard to 5G.

And that's it. That's it from my side.

Thanks.

ALEJANDRA REYNOSO: Thank you, Rafik. As I said, let's go through all our reviewers first, and then questions will be answered later.

KC, please.

KC CLAFFY: Hi there. Yeah, those were great presentations. I really appreciated the work that went into them and I'm especially interested in the SPIN work that SIDN has -- is putting effort into.

I'm curious about what folks know about government support for this sort of activity. I know in the United States, NIST has been working in this area for years, I think seeing an oncoming train and wanting to help industry get ahead of some of these problems. What I see is that the IoT movement is forcing a -- or will force, maybe we haven't seen yet a confrontation with a failure to overcome many of the fundamental security challenges embedded in Internet architecture. And we've spent a lot of time and energy developing technologies like DNSSEC and BGPSEC where standards organizations try to build a protocol enhancement that would solve a specific security problem but require global deployment that unfortunately hasn't really happened.

Alternative approaches have been to try to propose operational practices like, for example, in the BGP space, MANRS, which stands for

Mutually Assured Norms Regarding Security. Basically a code of conduct in the ISP world of if you do this certain set of things, you'll reduce the attack surface of routing security vulnerabilities that are built in that we haven't been able to overcome. This technical means.

I'm wondering if the panelists could talk a little bit to whether they think something like that is valuable in the IoT space that since in the IoT space it's not even an option to create a technical overlay the way we've tried to do in routing and naming protocols since there's so many different IoT protocols that aren't, you know, interoperable. So I'd be curious about some thoughts on that.

That's all I have. Great work, guys.

I'll put some URLs in the chat of the NIST work.

ALEJANDRA REYNOSO: Thank you very much, KC.

So, experts, who would like to start?

ELIOT LEAR: This is Eliot.

ALEJANDRA REYNOSO: Go ahead.

ELIOT LEAR: First of all, great points by all the reviewers, and thank you for -- and a great conversation in the chat room. It's actually a very engaging discussion.

KC is exactly right that NIST has been spending a lot of time and effort to address IoT security a challenges, and they are varied and many. So there is, for instance, the NIST TR8228 which talks about considerations for managing Internet of Things, cybersecurity practices and risks. There's also a draft recommendation SP1800-15 which looks at managing denial of service attacks in IoT with a focus on manufacture usage descriptions.

One point, and then I'll yield the floor, which is that IoT is not -- is a very nebulous thing. It hits different verticals different. We've been focusing a lot on consumers, but there's industrial, there's smart city, there's healthcare. And it's important to recognize that many of these verticals are already highly regulated.

And to give one example, the FDA regulates all therapeutic medical devices, regardless of whether there's Internet connectivity or not, they're regulating, and they're going to have a lot to say about the security of the device. And the same is going to be true for other critical infrastructure. IoT hits, you know, the nuclear industry. Of course that's highly regulated.

The question is what sort of regulation or best practices are required for so many other areas where we're seeing new uses of IoT that maybe are more reliably regulated. Even consumers have a regulated space but it's more likely regulated.

Thank you.

ALEJANDRA REYNOSO: Thank you, Eliot.

LISE FUHR: Hi, I'm happy to go next, if you want.

ALEJANDRA REYNOSO: Yes, Lise.

LISE FUHR: To Philippe, how to best reach out to the question on different players, I think the cooperation or the report from SSAC is a very good example of how we, as telcos, can use those to go back to our customers, business to business, but also to governments and others and discuss best practices and how to best make things secure. So I think the dialogue between those, ICANN and SSAC, and in Europe we have ENIS (phonetic) and ETSI. I think this is important. So that crossover needs to be done. And as ETNO, we're actually doing that crossover and uses this.

To Rafik, if there is any policy in the area on DNS and 5G, there is a lot of policies around 5G and security in Europe at the moment. And we have a new security act, which is also in relation to 5G not as DNS specific, but I think the more 5G develop, the more it will actually have a focus also on how DNS and IoT is -- is taken into the security area.

And we have what we call a 5G security toolbox, which is very much on the devices, but I think this is an important regulation that actually also will look into areas on DNS.

To KC's, on failure to overcome security problems, it's true. It's an area that is constantly in movement on how we deal with security because technology is developing really, really fast.

In Europe, we have ANISA which is a security body from the commission side. And they have actually -- they have now established a stakeholder security group with all the stakeholders that shall discuss standardization in relation to security. And I'm absolutely sure areas around IoT and DNS will be a part of this discussion, too. Thank you.

ALEJANDRA REYNOSO: Thank you, Lise. I suggest we -- yes?

CRISTIAN HESSELMAN: I just wanted to respond to what Rafik said about the role of the user.

ALEJANDRA REYNOSO: Please do, Cristian.

CRISTIAN HESSELMAN: We haven't touched that yet.

I think obviously users are an important part of the equation because that's ultimately what we all do it for. And I think we need to somehow empower users to better understand what's going on in the IoT so that they are more aware of what happens when they interact, when they consciously interact, with an IoT device which, for instance, could be a visualization or some other representation of their personal information that they're currently sharing with remote services on the Internet. And that might actually spark a discussion or a customer demand, if you will, for these kinds of security solutions in which the DNS could play a role.

Also, I think that the -- from a, you know, citizen perspective, which is also end users, I think that governments and other policy bodies also need to play a role there. And I'm already seeing that this is happening. So in the Netherlands, for example, the Dutch telecommunications regulator is quite active in that area. Like the NIST, for example, in the U.S. And we're also seeing activities around this -- around the radio equipment directive in Europe that I spoke about previously. So I think that ultimately it will also come down to policy where folks of governments and policy bodies like ICANN perhaps basically set out the standard for the minimal level of cybersecurity that needs to be installed on IoT devices.

Thanks.

ALEJANDRA REYNOSO: Thank you very much, Cristian and everyone.

Now, we will go through the questions that have been inserted in the Q&A section. Please be reminded to use the Q&A pod for your questions. Chat will not be read out loud.

So how are we on the Q&A? Ria?

RIA OTANES: Hi, Alejandra. We have a question from Angie Matlapeng: Has there been perhaps a workaround memory issues presented by much smaller IoTs, such as wearable devices in relation to using DNSSEC and encryption to protect devices?

ELIOT LEAR: Maybe I can take a swing at that?

ALEJANDRA REYNOSO: Go ahead.

ELIOT LEAR: Angie, thanks very much for the question. IoT has a couple of challenges in relation to encryption and memory usage. The first of which is obviously when you talk about consumer devices and other small devices in particular, memory is at a premium. I literally have debates with IoT developers over any bytes.

And if you look at the stacks they use, they are specialized encryption stacks, such as OV SSL is a good example where they have highly optimized encryption stacks. If you look at the size of open SSL, it can go into well over a megabyte in size. Whereas, OV SSL starts at about 14 kilobytes just to give you a feel for the differences.

But there's another sort of budding concern with IoT which is these devices, as somebody mentioned earlier -- Cristian mentioned earlier in his introduction, they last a long time.

And encryption -- the world of encryption changes over a great many years. What we thought was acceptable encryption five years ago, ten years ago is highly vulnerable to attack. And if you think about devices like oil derricks and oil platforms that you drop the device into the ground for 40 years, imagine what -- don't imagine. Remember what we had 40 years ago in terms of technology. And now imagining trying to update a device to use current technology. A device that's 40 years old, imagine updating a 40-year-old device. This is a big challenge for IoT. And it's not like there are simple solutions.

One person, I think it was Dan Gear from M.I.T., had a great paper that talked about, one, suggesting that IoT devices have essentially a kill switch where they no longer are on the net. Obviously, there are going to be times when that is possible and times when it is not possible. But it is food for thought. It was a great paper. Thank you.

ALEJANDRA REYNOSO: Thank you very much, Eliot. I believe we have one more question.

RIA OTANES: Yes. For the next question, do you think -- from Anupam Agrawak: Do you think the existing identifier system will be able to cater to the privacy requirements in case of IoT?

ELIOT LEAR: I think you're hearing a lot of silence because it's a very difficult question to answer.

Cristian, please.

CRISTIAN HESSELMAN: We spoke about -- actually, I think there are two parts. One is the identifier system which in this case -- is what we are talking about is the domain name as an identifier. So that can be protected to increase user privacy. We spoke about that early on in the talk.

But, of course, there is a second dimension, which is what kind of information are your devices sharing with remote services, right? So it can be about the actual content, but it can also be about the traffic patterns because there's been research where people would be able to assess what type of device you would have in your home base. Just by looking at the pattern of the traffic and not so much about the content of the traffic.

So I think there are various dimensions that need to be looked at if you want to increase user privacy. So it's about protecting the messages that we use for the identifier system, in this case the DNS. But it's also about the actual traffic that's being exchanged, that you send to remote service or that you receive from it to protect that information, both in terms of encryption and perhaps even in terms of obfuscation where you kind of try to hide what kind of device is basically interacting with the remote service.

I agree with Eliot that it's a complex question.

[Chuckles]

ALEJANDRA REYNOSO: Thank you very much, Eliot and Christian. Eliot, I don't know if you want to say something else?

ELIOT LEAR: I was going to try to answer Nigel's question. He asked about the challenges to I.P. as delivery mechanism for 5G in an IoT in standards world.

I think there are some challenges for 5G. The principal one is how do you limit the threat surface of these devices? How does the provider -- what's the role of the provider limiting the threat surface? And how -- what's the interaction between the network control point -- that's essentially a packet filter -- and the DNS in a cloud-based world?

And the same issues that I talked about in the home are also issues that have to be addressed by the 5G community. And we've begun to have those discussions, but we're just at the beginning of that point.

ALEJANDRA REYNOSO: Thank you very much, Eliot.

We will have one last question because unfortunately we are running out of time.

Please, Ria.

RIA OTANES: We have a question from Suada Hadzovic. If we have IoT cloud providers, what's about relation with mist, edge, fog nodes? According to NIST, fog nodes are either physical components like gateway, et cetera.

ELIOT LEAR: Okay. I guess I'll take a swing at this, too.

ALEJANDRA REYNOSO: Thank you, Eliot.

ELIOT LEAR: Thank you. I tried once already to answer this. So there are different computing models for IoT devices.

As I said in one of the answers, the cost of goods and services on the actual node, if we can -- the manufacturers try to keep those very low.

But sometimes you want to have -- so what they do is they move a lot of the Mule horsepower into the cloud which is highly scalable. If cloud -- if the manufacturer or the service supporter needs more, they can add more as they scale up. Cloud is great for that.

Where cloud might have some limitations is in latency where you want -- where you need local capabilities. And so that's this notion of fog computing.

I would say that it is an area that needs a little bit more exploration. It's not something you would see in the consumer space, but you will see a lot of fog computing in the industrial space where you have local controllers that are providing additional capability in terms of doing processing locally and coordinating of communication between IoT devices.

There's a lot of that already in the industrial space, but it's also an area that is ripe for exploration.

ALEJANDRA REYNOSO: Thank you very much, Eliot.

With this, I will wrap up what has been said in a very few sentences. It is very important for us to keep the conversation going regarding the opportunities, risks, and challenges that result from this interaction of the DNS and the IoT.

It is important to be aware that there is a passive interaction. That means the user is not aware of what is going on with their devices. It is something to work on.

Privacy is an issue, and security is an issue. There is some challenges regarding those. And the work that the ICANN community could focus on is understanding a little bit more on these risks and challenges and how the different community organizations and advisory committees can contribute to have a better interaction between the Internet of Things and the DNS.

I want to thank all our panelists and reviewers for their type and collaboration as well as all ICANN staff who have supported this plenary. Great job, everyone.

This plenary has come to an end. Thank you very much for your attendance. See you in the next one.

Bye.

[END OF TRANSCRIPTION]