DNS Security and Resilience

October 29 2024

Internet Society

DNS Security and Resilience – 29 October 2024

Claire C. van Zwieten - Internet Society Foundation: so, welcome everyone. Awesome, okay, there we go. So, welcome everyone. Thank you for joining us today for this very important webinar on DNS security and resilience. This is co-hosted by both ICANN and the Internet Society, and all of our panelists are mutual alumni, so they are all alumni of both the Internet Society and ICANN.

I bet many of us know DNS, Domain Name System, and it serves as the backbone of the Internet, it connects users worldwide to information services, but they are a target of cyber threats. It is important that, as a community, we understand what are the threats in DNS security and how we can be resilient, and, most of all, the role of multistakeholder organizations in making sure that we can thwart threats whenever they come.

Before we start, I would like to invite Jadiel who will be talking a little bit about our Pulse program and the Jadiel. So, Jadiel, if you want to come and start.

Jadiel ADEFOULOU - Internet Society: Okay, great. I'm Jadiel Adefoulou, I'm a data engineer consultant to Internet Society. It's a pleasure for me to come here and talk about the Pulse platform.

So, firstly, what is Internet Society Pulse? It's important to know that Internet Society Pulse consolidates trusted third party Internet measurement data from various sources into a single platform. We use the data presented to examine Internet trends and tailor data to the needs of users.

We use the data presented to examine Internet trends and tell data-driven stories so that policy makers, research analysts, network operators, civil society groups, and others can better understand the viability, evolution, and resilience of the Internet.

So, on Pulse, we track Internet shutdowns, estimate the economic impact of a shutdown using the Pulse Net Loss Calculator, measure Internet resilience, track the number of Internet exchange points around the world, and offer a country report, an easy way to get an overview of the state of the Internet in every ISO country in the world.

So, what about the DNS specifically? Two in three country codes domain are secure with DNSSEC. One in three Internet users are protected by DNSSEC validating resolver. Another statistic about DNSSEC, you can say that some country, such as Sweden, have a provider incentive for DNSSEC adoption. Consequently, we see relatively high level of naming security coverage.

Most Internet domains have very low level of DNSSEC adoption. For example, dot com domain is only 4% signed.

Claire C. van Zwieten - Internet Society Foundation: Thank you, Jadier. Thank you so much for educating us about the Pulse program and about DNSSEC.

Now I would like to invite our panelists for this webinar. We have Jackie Akello, we have Kanaan Ngutu, we have Lia Solis, and we have Marko Paloski. Thank you all for joining us today. Kanaan, I know it is thank you so much for joining us. I know that it is a quite early morning for you. It's probably around 3 a. m. in Kiribati, so thank you so much.

I would like to provide all of our panelists an opportunity to introduce themselves and share a little bit about what is their take on the current state of DNS. Lia, would you like to start?

Lia Solis Montaño: Good morning everyone. I am Lia Solis. My background is technical. I work at ISP. A lot of years. I work with DNS for ISP, in DNS resolvers. I love this environment of DNS, and I am systems engineering. Thank you.

Claire C. van Zwieten - Internet Society Foundation: Awesome. Thank you for sharing.

Marko, would you like to go next?

Marko Paloski - Netcetera: Yes. Thank you. Hi, everyone. I am Marko Paloski coming from Skopje, from Macedonia, and I work as a system engineer in one private company, more on the infrastructure part, but besides that, I'm also coordinator of the Internet Governance Forum North Macedonia chapter, and I've been part of the Internet Society fellowship, and also of ICANN Next Generation And fellowship.

So, I would say that's more or less for me. As a tech person, I'm more interested in the cybersecurity, privacy, online safety, Internet fragmentation, and platform regulation, those kind of topics. But yeah, thank you very much.

Claire C. van Zwieten - Internet Society Foundation: Thank you, and I love that Marko once again highlights that everyone on this panel is both an ISOC alum and an ICANN alum. They are all experts in this field and have taken the best fellowships in the industry to prove it.

So, jackie, can you please introduce yourself and share what your opinion is on the current state of DNS?

Jackie Akello - Research ICT Africa: Okay, thanks so much for that, Claire.

Hi, everyone. It's a pleasure joining you on this call, it's six o'clock in Nairobi. It's almost evening over here, or rather it is evening.

I am an AI Research Fellow at Research ICT Africa, and my work strongly revolves around AI and data governance. I mostly do research and policy analysis on topical issues that emerge from AI and data governance.

Other than that, I've also been privileged to be an ISOC fellow, so I was part of the 2020 cohort, and I got to attend the IGF through the fellowship. I've also been a fellow with ICANN for several times, so that is the ICANN 73 meeting and ICANN 77 meeting.

It's a pleasure joining you all at this call, and I'm looking forward to hearing your opinion and even just beginning the conversation on the DNS security. Thank you.

Claire C. van Zwieten - Internet Society Foundation: Thank you.

Kanaan, would you like to introduce yourself and share a bit about what you're up to professionally, and what your take is on the current state of DNS?

Kanaan Ngutu - Digital Kiribati: Yes, absolutely.

First of all, it was, it is a pleasure for me to join this conversation, despite the fact that it is very early in the morning in this side of the world.

My name is Kanaan, and as you already mentioned before, we are all part of the ICANN and ISOC alumni. I attended two ICANN meetings and also two ISOC meetings in the past, and right now I work on a number of stuffs. I do consulting works in the ICT space, I also work with ITU on the smart island projects in Kiribati, but at the same time I'm also leading an NGO called Digital Kiribati that's worked to promote cyber security and digital literacy within the community here in Kiribati.

Claire C. van Zwieten - Internet Society Foundation: Thank you.

I think something I want to share is, what's very special about this group is that they all are from very varying stakeholder groups. They all have a very different opinion and different view of DNS security and resilience.

I'd love to start with you, Lia. What is the role of DNS security and resilience in the work that you do, and what is your take on where we stand in that space in October, 2024?

Lia Solis Montaño: Okay. DNS is a service with a defined function which is to translate domain names into IP addresses. With these addresses, the packets can follow the best path defined by the routing equipment. Can you imagine a world where all users have to memorize IP addresses?

Precisely, one of the factors that has promoted the growth of the Internet in general is the ease of use, thanks to DNS. DNS is a critical service for Internet accessibility, therefore it deserves special attention in security contexts. To name a few, we can mention poisoning in queries where the origins of DNS responses are changed and contain false information to manipulate the destination of the packets.

The technical community has hard work for to avoid these threats.

Claire C. van Zwieten - Internet Society Foundation: Thank you. And you mentioned the technical community, and that wants, that makes me want to go to Marko. Based on your work and what you do, how do you feel that DNS has changed maybe over the past 10 years?

How have the security risks, and our models of resilience and DNS changed.

Marko Paloski - Netcetera: Yes. Thank you for the question. I would say even in the last two or three years, what has changed, not just 10 years, because in today's world, every year we have a lot of new challenges and opportunities and new technology, new versions, everything is changing and going in a better direction.

But yes, I agree, it's a good question. We also, as a people, are a little bit more aware of the things, because we use now the technology every day and more and more, but on the other side, because of the use of some of our skills, we are still lacking the knowledge -- or maybe not knowledge, but maybe to have the focus on the things.

That's why, in the last years, I think we have more and more cyber threats, especially on the DNS side. Different kinds of attacks. This is rising because, we are more dependent now on the technology we have in every device. Even now in the cars, we have technology and system and a computer, which that makes us more a target to attacks, in the 10 years before it was maybe the targets were the institutions, maybe the companies, the governments. Now, still they are target, but now also the end user is a target a lot.

It's a challenging time.

We are having more awareness now, because there is a lot of initiatives. Of course, some comes from Internet Society. ICANN also is doing much work on this for the DNS security, but I still think that we are far away from that we are always safe. The DNS, it's a critical system, but it's one of the most targeted, I would say, because as Lia mentioned, it's one of the core things of the Internet.

You cannot imagine Internet without the DNS, especially the DNS security, which today it's by the default. In the past, maybe you didn't need to have DNS security extensions or some kind of things, but today you cannot go without that.

So, I would say with the advancement of the technology, also the advancement of the attacks and of the vulnerabilities are going -- we have now artificial intelligence, you can ask GPT to write, or to give you some vulnerability of some site, or maybe to make you a tool.

On the one hand, it's nice because you can see and test more of the systems because you can see how the machines are working, but also it gives a lot of power to some people or with bad intentions. Maybe they don't have bad intentions, but when you have the tool, you can try it.

So, yes, it's challenging, but our work is very crucial, from the tech people, but also not the less from the policymakers and all other people, because it's the topic is important. Multistakeholderism here is one of the crucial thing, because I think the Internet is based on the multistakeholderism and it should continue on that. Each stakeholder, their work is very crucial, especially to these times where we are now facing.

I don't know if I directly answered the whole question or a little bit go in the outsides, but I wanted to try more to give some answer.

Claire C. van Zwieten - Internet Society Foundation: You definitely brought up a very important point, which is that the more our lives become increasingly digital, they are equally vulnerable as much as they're increasing, because as much as our lives, as you said, in our cars and everything, we have a computer these days, so it makes sense that as our usage of these things increases, so does our vulnerability.

And Kanaan, I want to go to you, because I know you work a lot with the community in your area. And, since you do a lot with cyber security as well, I'm curious how you've been able to talk to the people in your community about this topic, and if you've been able to find ways to bridge a technical gap for people who obviously know about the Internet, but they don't necessarily know about the infrastructures in place that keep it as safe as it is.

As Marko said, you can't have the Internet without DNS, but many people don't know about it, actually. So, when talking to your community about cybersecurity, how are you able to fold this in?

Kanaan Ngutu - Digital Kiribati: My discussion on this topic would be revolving around the Pacific experience, coming from the South Pacific.

We know the DNS as it is, and its role in the whole infrastructure of the Internet. It is one of the crucial elements that needs to be protected. DNS, we know its importance, as it can determine the fate of the Internet, and in order for the resources to be accessible on the Internet, we need this critical element.

This is especially true in the Pacific Island context. We've been operating from the other side of the world, practically unknown to mostly everyone in the Western world, but dependent entirely on the Internet, and, we have stakeholders that involves in shaping the Internet as it is, and, going forward.

But, sadly, most of the people, especially the people that's supposed to have a role in maintaining this resource, do not necessarily know this critical element of the Internet, right? I think it speaks to the fact, the importance of getting more and more people to involve, and I think engaging the people would start At, building the capacity for these people.

As you rightly mentioned, I learned a lot of things, and one of it is that most people lacks the knowledge of DNS. They do not even know what are the vulnerabilities, what are the security threats that undermining the DNS operations in the Pacific, and when you talk about cybersecurity, people in my community tends to be very vulnerable compared to people from other side of the world. Partly because the Internet, it's relatively new in our horizon when we compare to some people that located maybe in the US or in Europe.

You can imagine using the Internet for the first time, with its vast resources. People believe that the Internet is a really good thing, that is the fact, but they do not know what are the threats inside the Internet. There are things like online child abuse, the scams and the attacks that it's been conducted on the networks, and on individuals as well.

So, these are the things that people in the Pacific lacks knowledge about, and make them all the more vulnerable to this kind of attacks. It is the same when you consider with DNSSEC, and I believe people would realize when they came under attack, that is when they will realize the need to upskill and stay informed and engaged in this very important arena.

Claire C. van Zwieten - Internet Society Foundation: Thank you for that answer. I love what you said and I think that you make a great point when you talk about capacity, is that people don't know what they don't know, and if they had the resources to be able to learn best ways to protect themselves then it might be easier for them.

Luckily now in 2024 we have AI, and that is providing a lot of new opportunities to build the capacities of people in a lot of different realms. I would love to jump to Jackie, and see if she could bring us any kind of information or insight into the role on AI and DNS, and if people are using artificial intelligence to help either teach themselves, or to keep themselves safer.

Jackie Akello - Research ICT Africa: Thank you so much for that question, Claire. My colleagues have shared very important insights on the security of DNS, and also just on the state of the DNS currently right now in the globe, so I'll share some insights on what role AI plays, particularly in just keeping the DNS system.

What you've seen recently, particularly in the past years, AI has really grown and right now we have generative AI and ChatGPT. The role that I see AI play, particularly in the African context and also just people in the grassroots level and in the education systems, is that it now educates people on the DNS systems. People get to see how crucial the DNS system is, how it works as an infrastructure, and also just get to understand the crucial role that it plays.

Another thing is that AI also, just through the educated tools, is that it exposes people to the harms that can be posed on the DNS systems. People know that, okay, in as much as the DNS infrastructure is a critical infrastructure, just people communicating and even just reaching out to each other, there are harms that exist when using other systems, and they're also equipped with information on how they can protect themselves.

Another thing is that AI is also being used to cause insecurity in the DNS system, so things to do with cybersecurity, harms, and even attacks, are just created just by the use of AI systems. This is a crucial risk that actually needs to be addressed in terms of looking at DNS systems and AI.

AI also plays a crucial role in terms of policymaking around the DNS systems, because it brings about crucial stakeholders who are involved in the development of these AI systems, and also sharing of knowledge on how some of these harms can be prevented and also mitigated.

So, AI has a crucial role to play in terms of DNA security, and also the advancement of policymaking around the DNA system.

Claire C. van Zwieten - Internet Society Foundation: Thank you. That was a great answer. I think that it's really important that, your everyday people, the cashier at the grocery store, your mom, your dad, that they all, everyone know how to protect themselves and best practices for DNS security.

If you could tell, I would love for every one of our panelists to answer this question, if you could give one practical piece of advice to people who want to protect themselves and make sure that they are maintaining a resilient system that has robust DNS security, what would you suggest to them?

And we can start with Lia.

Lia Solis Montaño: We can talk about the best practice, for example. It's important to understand the recommendation for the deployment and operation of the name resolution service, but also to be open that this recommendation are dynamic operands based each threat identified on the Internet.

We can cite some best practices, for example, have authoritative DNS and resolving DNS in different infrastructure tools, ensure redundancy of the DNS servers in the most transparent way for the user. One of them may be to use of anycast clouds, in which it allows us to have the server with the same IP identifying different geographic locations.

Other, carry out good dimensioning of the infrastructure based on the traffic generated by the network users. These measures specifically restrict recursive queries to the IP addresses of target user, ensures the veracity of responses to queries loading in DNSSEC?

The best guide to KIND DNS is to refer to the learning platforms provided by ICANN, and also the Internet Society, regarding these topics.

At this point, I'd like to add that all parties must understand that the DNS is not a tool for blocking. This is a very broad topic that may raise it for another webinar, but I consider important to mention it to lead the multiple actors thinking.

Thank you.

Claire C. van Zwieten - Internet Society Foundation: Thank you, and thank you for sharing that both ICANN and the Internet Society both have great resources on DNS security, and the best guides that you can get to protect yourself. Thank you for sharing that, I think it's important for the audience to know.

And then, Marko, I would love to hear your answer as well of what are best practices in DNS security, and what can the average Joe do for themselves to protect themselves.

Marko Paloski - Netcetera: Yes. Depends on the system, of course, but there is a lot of best practices. As you mentioned, there is a lot of from Internet Society and ICANN that are helping you choose or find what is relevant. Because, not always the organization, the company, or the individual, has the knowledge or the resource, doesn't need to be that resource is only money, but people with knowledge who know what to do.

From the technical point of sight, implementing of DNS Security, DNS secure, 10 years ago, maybe that was like an advantage feature or something like that, so high level, but today I think it's one of the basic stuff that you must in some way implement, if you want to have a secure DNS or secure system, because DNS is one of the core things that if the hacker gets to that one, your company or your organization is vulnerable and open to attacks, open to a hacker.

There is a lot of other things that some of them maybe existed in the past, some of them maybe not, but during this rise of the new technology, everyday use, a lot of them are specified and maybe advanced, so I would add more on monitoring and log the DNS traffic. Especially with AI today, there is a lot of systems that can see the behavior of the network, see the requests, those kind of things, but also manually checking and seeing because, as the defending machines or artificial intelligence is rising, also the attacker is rising. Both sides are good and bad, and always, when one side advances, also the other will advance after some time.

There is a lot of blacklists applying rate limitation, how much requests in a certain time can be sent or received, or maybe processed. Depending on the systems, we can see that, especially when DDoS attacks are happening, a lot of companies, sites, are doing limitation in period of time, how much requests you can do, which I think is very smart and nice thing to implement, depending on the system, and what is the purpose.

Then, to have redundant DNS servers, DDoS attacks, the whole idea is to shut down or take off the ability of the server, so if you have redundant, it's maybe better infrastructure in a sense, or resilient.

Always, also for the end user to have all the updates, or the application up to date, the operating system, the BIOS, the network, the switches, depends how big and what is the company, but everything to be up to date. This is a easy and and small thing, but many times people forget to do those kinds of things. Especially, only for our phones when we don't update it or we forgot to update the application, but if you see in the history of the attacks, or what happens or some that got publicity, we can see that a lot of the things were, some software was not updated, something was older version, and those kinds of things.

Of course, not always can you be up to date, because of certain limitations or application that you're using, but still it is a crucial thing. If you see that some software was not updated, I will still track it down to a person, a mistake, because someone needs to update, that it's not like AI automatically to update. So, most of the attacks that have happened are mistakes from the employees, or the people that are maintaining or doing the job on the servers.

There are a few more things. Blacklist, also DNS filtering. That is also happening from time to time, which sometimes in the good use, but sometimes in the bad use that are some countries or regions limited from accessing or sending. In a good sense, I tell that you can limit if malicious, or specific requests are coming, but in bad times that, as someone mentioned from the panelists, DNS is not a way to block the Internet or to block access, but to give access. We can see in some cases that sometimes DNS is used that maybe country states, they are using for blocking.

And, yeah, always access control list, and maybe limiting zones for transfer. This is more specifically for technical parts, where transferring of IP addresses, or which you can take a new one or something like that.

Those are five, six, seven that I mentioned, but those are the basic ones. There is a lot of more complicated, and I know that also in work we have some kind of software, that I didn't know that this kind of sophisticated restriction you can apply, but it makes sense after you see what kind of attacks are coming.

So, you always try to protect from any kind of threat, even if it's not threat, just to be protected, because sometimes, maybe tomorrow, it will come as a threat, even if today it's not, so I will give those as best practices.

Claire C. van Zwieten - Internet Society Foundation: I do want to quickly, while we have you, Marko, share a question that was asked in the chat by Sana. She says, Thank you all for sharing your important knowledge with us. You mentioned the importance of multistakeholder collaboration in DNS security. Please share your thoughts on specific practical steps that different stakeholders such as private companies, government agencies, and technical experts can take to enhance collaboration in securing a DNS system. Are there particular areas where teamwork can be improved in both existing and emerging threats?

I would actually like for as many of our panelists as comfortable to share what their take is on that, because it's a great question. So, Marko, since the question was directed to you, would you like to answer?

Marko Paloski - Netcetera: I can say that it's very good question because sometimes, especially in the DNS correlation, when you ask about companies, because also I work in a private company, it's not that much understood, because if they understood what the benefits this multistakeholderism can have, I think everyone would want it. Of course, sometimes it's a lack of knowledge of how this thing is working.

I think that multistakeholderism is a very good approach, especially in this topic, because the Internet and Internet governance is based on that, especially when, as you mentioned, private companies, government agencies, technical experts, not always those kind of corporation institutions have the resources and knowledge.

Maybe some institutions have very good knowledge in cyber security, someone else, they have maybe the software, but they don't have the resources, and it's very crucial to have a cooperation and communication between them. Also, I'm coming from a small country, Macedonia. We have a CERT, but it's very small, and it's not that much prepared for a big attacks or something like that.

Often what I see is sometimes that the companies are helping the government or some organization to help mitigate those kind of attacks. Unfortunately, there is not a global platform for every country, or every company, can join, but there are a lot of initiatives that are going on that also individual or government or private company can.

It's very nice to mention, here, because we are a part of this webinar, I can point out that there are a few organizations that are doing different kinds of things on multistakeholderism, for best practices and also standards setting. ICANN is doing a lot, also the Internet Engineering Task Force are developing the standards, they are developing best practices, you can find on the site.

Internet Society is also one of them, together with ICANN in policy advocacy, raising awareness. There are a lot of initiatives from Internet Society people can join, and there is also a network of experts where you can share or ask on the forums. There was DnS Abuse Institute, but now I think they changed the name, it's more about incident response and mitigation and collaboration on those kind of things.

So, there are many platforms or maybe forums that can be useful for companies, organizations, and those kind of things. For organization, I wouldn't say that much, but for companies and governments, I see the lacking of benefit of joining or using that much.

The company, sometimes they say no, we can't pay someone, we can solve this, we don't want to collaborate, or sometimes the company doesn't want to share what happened, even publicly.

And the government is, depends on the government, of course, sometimes they want just to make by themselves. We had the case in our country where it was attack the server, but in the end it came up that they were the one who organized that, to steal or launder money .

So, sometimes it's a problem, but it's a very crucial thing, because if everyone is cooperating, it will be much more easier to mitigate attacks and also to be more safe and secure.

Claire C. van Zwieten - Internet Society Foundation: I agree with you, what you say about when governments will just try to do it within the government. Of course, they probably have a whole various and variety of different skill sets within that government, but really nothing formative, nothing true, robust change happens alone.

So, I really would like to bring up Jackie and ask her what her opinion is on the multistakeholder approach to DNS security and resilience, and where there are increased avenues for collaboration which should probably be explored.

Jackie Akello - Research ICT Africa: Thank you so much, Claire.

Multistakeholderism actually plays a very key role in the security, and also just the resilience of the domain name systems. These organizations bring together various stakeholders, and these include governments, they include private entities, the society organization, and also just technical experts.

When these organizations come together, what they do is that they ensure that diverse perspectives, and also the interests that actually shape the policies, technical standards, frameworks are also shared, and they enable the governing of the Internet in a very meaningful way, in a very fruitful way that enables our DNS security.

The importance actually lies in maintaining an open inclusive and resilient Internet that reflects the needs of all users, while addressing the complexities of a global interconnected network.

I think multistakeholder plays a key role in the DNA security because of the unique values it adds in policy making. For example, it enables inclusivity and representation. What happens is that multistakeholder organizations actually bring together different voices from governments, the private sector, and technical entities. At the end of the day the inclusivity ensures that Internet governance actually reflects the diverse needs, and also priorities, rather than just favoring one particular group in the DNS ecosystem.

Another advantage that multistakeholderism has is that it enables transparency and accountability. Decisions on DNS made through multistakeholder processes are generally more transparent and accountable when various entities have been involved in the formulation of those decisions.

Organizations such as the IGF create open forums where policies and practices can be debated. They can be discussed and reviewed by people with different expertise in the

DNS systems. What happens at the end of the day is that people share best practices that can govern the DNS systems in the best way moving forward.

Another advantage of multistakeholderism is innovation and responsiveness. As we all know technology advances at a very fast pace. So, when you involve people from different sectors of, for example, civil society organizations, what happens is that people share their experience and even their expertise on the current technologies that we have, it ensures that the current laws that we have, are also in tandem with the advancement of technologies.

People get to share what's happening in the tech space, what new technologies are being launched, and what policy considerations and measures need to be put in place to ensure DNS security.

Another advantage of this is that, at the end of the day, all interests have been considered, so it ensures that there's a balance in terms of the interests that are presented in debating the DNS issues. We get different sectors, we get the civil society, we get the government and policy makers. When they are all put at the table, and they discuss and they agree on key issues, what we get at the end of the day is that their interests are balanced, and everyone has been catered for in terms of the the opinion they have on DNS security.

One final thing I can say about multistakeholderism is that it also builds trust and legitimacy in the system because all voices have been considered. Everyone has been able to share what they think in terms of the policy making on the DNS and even the security of the DNS.

What happens is that whichever rules and policies are passed at the end of the day, they can be regarded as being legitimate because everyone's voice was considered in the development of these policies, and everyone's view was also considered.

So, what we get at the end of the day is that it ensures that there's legitimacy as compared to just having a secluded group that's making decisions on DNS issues, and also just passing policies. When that happens there's a lot of mistrust, and people don't regard those policies and even those decisions as being legitimate.

So, in a nutshell, I can say those are some of the advantages that we have around multistakeholderism in the system.

Claire C. van Zwieten - Internet Society Foundation: Thank you, and thanks for bringing up the important aspect of trust by design. when we develop policies and we develop systems with safety and trust in mind, that has a ripple effect, through the users, through the community that is using these systems. So, thank you for bringing that up and also shining a light on the policy side.

That's a perfect segue to looping in Kanaan again. He is a policy consultant, and I would love to hear what your experience is when it comes to creating policies and consulting on policies such as DNS, and what kind of challenges and also opportunities you've seen in that process.

Kanaan Ngutu - Digital Kiribati: Again, speaking from the Pacific Islands, I want to speak within my own context, and I think the experience is similar with DNS and every other part, of the policy in other areas.

It started off with to get the stakeholders, that are supposed to be involved, to better understand what the nature of the work would be, and that is to ensure that they could contribute meaningfully to the discussion, and to shaping the policy aspects with DNS in the Pacific. As I mentioned before, not many people understand this.

I understand that there are a number of platforms created on the international stage that foster engagement in this area, but one of the main challenges that we have in Kiribati and in the Pacific Islands, we have a very different time zone with other countries.

So, that's clear that we need to create our own space, like a subspace, that would encourage local stakeholders to involve on the personal level. What I mean by this is, in Kiribati what we do is we try to identify champions, champions that would encourage artists to come on board and to discuss these things. This is where the support of ICANN and ISOC in producing the resources that we can use locally, and we can translate those things, just to ensure that the people with interest have a comprehensive understanding because that is where we will start to build the capacity from the local level.

As they become mature, or acquainted with the knowledge that's necessary, they could take this and bring the engagements to the regional level, and to the global or international level, in terms of, discussing matters that relate to the policy.

I think that is how we should start in the Pacific, and it also applies to other parts of the world that consider themselves isolated from the entire global community. You need to start within your own society and bring on the stakeholders and build their capacity, because from there you can ensure that, once they want to take their engagements to the next level, they will be able to be more meaningful and efficient in that aspect.

This applies to DNS, and it also applies to every fields where you need to develop policies and engage a multistakeholder model.

Claire C. van Zwieten - Internet Society Foundation: The role of champions in creating robust systems and policies that protect the Internet and defend the Internet is crucial. A little shameless plug here, that's something that was really great about ICANN and the Internet Society, is that we're able to have these programs that all of everyone on this call has gone through, and through that, you've been able to become champions of your own right, and champions of the Internet.

Whether it's technical or policy, or whatever it is, you've been able to go take these skills and go back to your community and implement them for good. It's important that we continue to be able to create and develop champions such as you four, so that you all can really do, honestly, the legwork of Internet defense. It's really you all on the ground in your positions, in your jobs, and in your life, really protecting the Internet and doing everything we need to do.

So, thank you all so much for everything you do, and thank you so much for everything that you've added to this conversation.

Before we have to close because of time, I would love to make it to the three questions we have in the Q& A and I'll start with first by Ryan Uddin. What vulnerabilities in DNS make it susceptible to spoofing attacks? Would you like to answer that one, Lia?

Lia Solis Montaño: Okay. When we have to verify the IP address, is we have to implement these spoofing methods in our infrastructure, and the principle for doing this is DNSSEC.

Claire C. van Zwieten - Internet Society Foundation: Thank you.

Then we have another question from Nicolas, who is one of the Internet Society alumni. He says, How can the KinDNS framework be optimized to support quantum-resistant cryptographic algorithms -- what a collection of words, wow! -- and DNSSEC, as advancements in quantum computing, such as quantum annealing, threaten traditional encryption methods like RSA 2048.

Nicolas, you are testing my ability to talk today. Wow!

So, Marko, would you like to take that one?

Marko Paloski - Netcetera: I would try because I'm not that much into quantum computing and those kind of the crypotography but I know that Nicolas is very much, because also last year at the IGF in Kyoto, he was also discussing and asking questions about this.

I'm not sure, but I know that this KinDNS framework, which is from ICANN, it's the whole idea that I previously speak about, multistakeholderism and a place for best practices, this is one example that ICANN is doing with this framework.

But, how to optimize about the quantum-resistant cryptographic algorithms? That's a good question.

Claire C. van Zwieten - Internet Society Foundation: You said that with such ease. You make it sound so easy.

Marko Paloski - Netcetera: Yeah, he's talking like a normal cafe chitchat, but, I think that the cryptographic, especially now with the quantum computing, we are still far away from those kind of big processing, but someday eventually we will be there. Quantum computing plays a big role now, especially in cryptographic for those that are less secured, because it'll be much more easy, with quantum computing for the time to decrypt or to find the encryption key.

This thing is relatively new. It's in the research, there is few commercial projects, that are actively doing this, but I think that more of the systems will get more advanced and it can become more easy to be implemented or optimized.

As I mentioned, I'm not really sure because I am not that much involved in this quantum computing, and especially encrypting with quantum computing, but my idea is that, with time, the systems will be more advanced, more easy to optimize, or configure with both things, because there will be more space for that.

Not sure if I answered. Knowing Nikolas, I know that it is not the full answer.

Claire C. van Zwieten - Internet Society Foundation: So unfortunately, Jackie has to drop off, but thank you so much, Jackie, for all of your insight today, and thank you for lending your excellent DNS and legal mind to this talk.

Now we have another question: What steps can be taken to encourage widespread adoption of security practices?

I would like to go to Kanaan for that one.

Kanaan Ngutu - Digital Kiribati: The answer is obviously, we have to make people more aware, especially the organizations. They need to be more aware of what the threats are, and also to guide them, and teach them on what measures to take in order to start implementing the securities around DNS infrastructure.

That is what is very important for me, because, as far as I know, with , a lot of organizations that I worked with, most people, even in the ICT department, they do not even know about how to take measures to protect their DNS infrastructure, especially in the specific context.

Again, their network is so simple, there is no sophistication in there, and so how can they implement DNS when they do not have a proper network infrastructure?

So, in order to encourage people to adopt and implement best practices, we need to educate these people, and show them how it's being done.

I think that from there they can build their knowledge moving forward.

Claire C. van Zwieten - Internet Society Foundation: It's a great question and a great answer. I'd love Lia to tackle this one as well, and I think that this will be the last question we answer before we have to unfortunately close the webinar. But Lia, I would love to hear from you on what we can do to increase adoption rates of DNS.

And the-- what was the other fun acronym? The KinDNS.

Lia Solis Montaño: KinDNS gives our standard guide to having DNS. It is what we can work with initially for those of us who want to find a guide. Good practices are dynamic and adjust to the needs of time. Certainly we can make contributions in each scenario that may arise. Remember we have communities concerned about this use.

Claire C. van Zwieten - Internet Society Foundation: Thank you so much. And I think that what some, what this person also asked about is what we can do to make sure that we're setting adequate security standards for these kinds of systems.

Do either of you have any insight on the importance or the ability to set standards?

Marko Paloski - Netcetera: Check the best practices, check what are some known things in the international, and from organization like ICANN or Internet Society.

Check also with your local country or community, what others, institution or governments, are doing, or if there is a law. I don't know about that, but still check it. Even if there is nothing, try to come up with something and see if it's good. If not, then change it.

Those kind of things are not just you make it and it's for life, you need constantly to review and update because technology changes, attacks changes, so it needs to be up to date.

That's all.

Claire C. van Zwieten - Internet Society Foundation: Awesome. And, on that perfect note, we do have to end this webinar. Thank you so much to our speakers. Thank you for taking time out of your day and early morning to lend your expertise and your time to share everything you can with us.

Thank you to all of our audience. Thank you for coming. I hope you were able to learn a little bit, and I look forward to seeing you all at our next event. We will make sure to share that when we can. I hope everyone has a great day.