DEVAN REED: Good morning, good afternoon, and good evening to everyone. Welcome to the AFRALO Webinar on Data Security in Tuesday, the 7th of September, 2021 at 18:30 UTC. We will not be doing the roll call, as this is a webinar. However, attendance will be noted from the Zoom Room as well as the audio bridge. We have French interpretation on today's call. Our French interpreters are Jacques & Isabelle. From staff, we have Heidi Ullrich, Silvia Vivanco, and myself, Devan Reed, call management.

Before we get started, I would like to remind everyone to please state your name before speaking for transcription and interpretation purposes and to please keep your microphones muted when not speaking to prevent any background noise. Thank you very much. And with this, I'll turn the call over to you, Bram.

BRAM FUDZULANI: Thank you, Devan. Once again, everyone, welcome on behalf of myself and my colleague, Tijani, on the call but also on behalf of the AFRALO leadership. This is one of the topics that was voted by the community members when the call was made out for us to prepare for the ICANN 72 drafting of a statement.

So I would like to take this opportunity to just thank your presenters, Yazid and Paul, for making time to walk us through this wonderful topic. Let me invite the participants to be free when it comes to Q&A. Let's ask questions where we are not clear—clarification. It's an interactive session. So I will give the floor to our presenters and then we'll go into the Q&A session after the presentation. Thank you so much.

YAZID AKANHO: Thank you very much, Bram. It's, again, my pleasure to be here with my family, AFRALO. And today, Paul is also part of the presenting team. Paul is also a technical engagement specialist for Middle East and Africa region. So we are both working in Africa and Middle East region. So today I'm going to present … Sorry. I do not have the sharing option. Can I get this option available, please?

DEVAN REED: Absolutely. I'm making you the cohost now.

YAZID AKANHO: By the way, can you also allow Paul as cohost?

DEVAN REED: Let me check for you. Otherwise, I'll [inaudible].

YAZID AKANHO: Thank you. I hope you can see the slides now.

UNIDENTIFIED SPEAKER: Yes. We can see it.

YAZID AKANHO: All right. Thank you so much. So today, we are going to present a very board topic, which is data security, of course. And we'll emphasize on

DNS data security, mainly. The topic itself is very large—very broad. Even DNS data itself is very large. We can even spend a full day on it. But we will try to go through some important aspects of DNS data security in the next 30 minutes. We do hope that, with your questions and comments, we will make this session very interesting.

So the agenda is quite simple. We'll do a kind of brief overview of the DNS. I still remember, for those who attended, we already had a session related to DNS last time. And then, we'll introduce DNS data security, looking at the global architecture of the DNS. And then, we will start going into some of the specific aspects of DNS data security, like DNSSEC, talking about DNS privacy, also RDAP. And we will end up with some of the ICANN Organization initiatives to actually support a secure DNS ecosystem.

So what is the DNS, very quickly? For those who attended the previous capacity building session related to DNS, we actually explained that it is a kind of phonebook for the Internet. It is the place where we actually try to match IP addresses and names. Why? Because humans are more comfortable with names but we are manipulating devices which actually require an IP address to be connected and to be identified on the world Internet.

Today, the Internet is composed of more than 100,000 networks. So we are talking about billions and billions of devices which are connected. The same way the Internet has been increasing in terms of number of devices connected and in terms of number of services which are connected—available for the users—we have also seen the need to have an hierarchical and more organized system to actually translate the IPs

into names and names into IPs. This is how the DNS was invented in 1983 by Paul Mockapetris and Jonathan Postel.

So the DNS is actually a hierarchy, with the entry point which is called the root, managed by ICANN. Beyond the root, we have what we call the top-level domains, the second-level domains, and etc.

So when we look at how a device actually tries to do the resolution process—because we, again, as human, we just type in the names. But the device actually needs to know the IP address which corresponds to the name we type in the browser, for instance. So the device actually talks to a stub resolver which is a piece of software embedded in the operating system. But probably, the stub resolver will not also know about the corresponding IP address.

So definitely, the stub resolver will query. We send a query to an external server, which is called the recursive name server—the recursive resolver. Usually, this server is located at the ISP premises or in our local network. The role of this recursive resolver is actually to query several authoritative name servers. Those authoritative name servers are the places where the corresponding—the relationship is done between names and IP addresses. So those authoritative name servers are just a reply. They give answers based on the configuration they actually have.

One the recursive resolver queries a lot of authoritative name servers and gets the final IP address, it reverts back to the user now with that IP address. And it is only once the resolution process is successfully completed that the user is able to query the websites by sending an HTTP or an HTTPS request to that IP address, requesting the website. So

here, you can see the example of some user using his iPhone go to icann.org website.

So again, if this DNS resolution process fails, unfortunately, the user will never get access to the website he is requesting. And also, there are other types of issues that may occur. And we will try to see this in the next slides.

Let us now introduce data security, quickly. When we talk about security, there are three major functionalities. There are three major functions that we want to achieve when we are talking about security, the first one being confidentiality. By confidentiality, we try to prevent all unauthorized access or use of information or data. The second one is integrity. How do we make sure that the information is not modified by any entity? And the last one is authenticity and availability. How do we make sure that the data—the information—is available to those who are authorized to have access to it with reliable manner?

And of course, the DNS has been victim over the years because the DNS, as an infrastructure, is an important point or an important infrastructure for the Internet itself. So we have seen, over the years, several attacks conducted to actually modify DNS data or to make the DNS unavailable—so DDOS attacks, some hijacking attacks causing modification of DNS data in the cache, for instance. We have also seen man-in-the middle attacks and other types of attacks—cache poisoning, redirections, etc.

So over the years, we have tried to see what are the potential target points of the DNS infrastructure. Without knowing it, we cannot try to give or provide protection mechanisms to this DNS infrastructure. So if

we look at the current infrastructure on the slides, the end user is considered to be behind the stub resolver, at the left side. So the stub resolver is always talking with the recursive. And we can have man-in-the-middle attacks or querying at this level.

In the recursive resolver itself, unauthorized people who have access to the recursive can actually poison the cache or modify the data. Between the recursive and authoritative, you can also get some kind of spoofing or man-in-the-middle attacks there as well.

And when you go on the authoritative name servers where the databases are actually stored—those databases which contain the IP addresses and the names they are linked to—people can try to corrupt the data. So getting unauthorized access, using different ways, different channels, trying to corrupt the data stored in the databases.

And those data which are stored in the databases actually come from where? They come from the registrants—the registrants who go to the registrar and try to register for a domain name. So from registrant, also we have seen different types of attacks.

Now, let us try to understand how we can secure the DNS infrastructure. Of course, we need to call different techniques, different methods. On the recursive server, for instance, we have to deploy what we call access control mechanisms. There are different levels of access control. Rate limiting also is a common mechanism to the recursive resolver side. On the authoritative servers, there are also plenty of mechanisms to ensure they availability, the security of the databases.

Now, when it comes to the DNS data itself—how protect those data—many of you know about DNSSEC or at least have heard about DNSSEC. In the next slides, we will see what is DNSSEC, deeply.

And of course, data are called to move from authoritative to secondary name servers. How do we ensure that we protect those transactions which are done between authoritative, or primary, and secondary name servers? So there are two major techniques there. The first one and well-known is TSIG. But there is a new protocol that has been published by IETF just a few days back, which is called XoT, XFR over TLS. For those who are interested, it is the RFC 9103. So now, we can configure secondary name servers to actually query the zone file from the primary server using TLS.

And of course, privacy and confidentiality, we have here the DoT and DoH since several years now.

So if we come back to this architecture of the DNS again, let us try to put each technique and mechanism to the right place. Of course, we will see also new words, like registry lock, here, which actually occurs at the registry level. Registry lock is actually a mechanism just to ensure that the registrant clearly gives authorization for any data modification related to its domain. We also have, like I said before, TSIG and XoT occurring between primary and secondary name servers. We have DNSSEC, DoT, and DoH, like said before. But we also have several techniques and projects which actually focus more on registrant security side.

We'll now try to go step-by-step into some of those mechanisms and techniques to understand what they actually stand for. Some of those

techniques are just DNS records themselves. So to secure the data, there are some DNS records which exist, mainly to secure e-mails. When it comes to e-mail security, ones who actually have a domain can define three types of DNS records to secure their e-mail infrastructure. Those records are called SFP, for Sender Policy Framework; DKIM, DomainKeys Identified Mail; and DMARC, Domain-Based Message Authentication, Reporting, and Conformance.

Those are just DNS records, like a record—like AAAA record. I won't go into the technical details but they are just some kind of methods to secure the e-mail infrastructure by defining, for instance, which e-mail servers are really authorized to forward or to send e-mails for this particular domain, etc.

When it comes to systems management, we talked about primary server. We talked about the secondary servers. All the registration systems are running, definitely, on some hardware or some virtual machine. So we need to ensure that all the patches are applied on a very regular basis. But how do we also access those systems and applications? So password and authentication engine must be in place. Later on, we'll talk about DNSSEC. So let us try to introduce you to DNSSEC.

For those who don't know, DNSSEC stands for Domain Name System Security Extensions. So those are new extensions to secure the Domain Name System. DNSSEC is actually a protocol deployed to secure the DNS. We have been using DNSSEC since 2005 now. So the latest standards of DNSSEC have been published in RFC 4033, 4044, and 4035, for those who are interested in reading about DNSSEC. So since 2005,

now we have been using DNSSEC. And the root of the DNS itself had been secured in 2010. In 2018, we did work with [technicality] called the KSK Rollover. So we changed keys, which actually secure the root of the DNS.

Of course, DNSSEC adds security to the DNS by using some cryptography and keys to secure the data. It actually signs the data. So why do we sign the data? To ensure authenticity and integrity of those DNS data. So the domain name registrants who want to secure their zone file or who want to secure their domain, they just need to sign their DNS data. They need to sign their domain.

But on the other side, there is another operation which requires DNS operators and ISPs to configure their recursive resolver to actually do what we call DNSSEC validation because on the one hand, we have to sign the domains. But on the other hand, we have to validate those domains which have been signed. So the recursive resolver must do what we call DNSSEC validation. Of course, DNSSEC actually prevents DNS threats and abuses.

So what DNSSEC does and what it doesn't do. DNSSEC will, again, use the cryptographic public-key, cryptography, and digital signatures to provide data origin authenticity. So we want to ensure that that data—the DNS record—actually comes from the right name server and this DNS record had not been modified by anybody, from the name server to the user. DNSSEC will protect against spoofing of DNS data but DNSSEC will not provide any encryption or protection against man-in-the-middle, etc.

There is an important aspect of DNSSEC, which is called chain of trust. It is actually to establish validation from the root—the validation of the record from the root to the data itself. Whatever is your position in the DNS hierarchy, we have to establish this chain of trust. At the technical level, there are some configurations to do. And you have to share some information with your parent. Your parent itself also has to share some information with its parent to … This is the way we actually establish this chain of trust.

Of course, depending on your position, your role, you also have work to do in this DNSSEC journey. So if you are a company, you have to sign your domain name. You have to enable DNSSEC validation in your resolvers.

For those who are interested in statistics related to DNSSEC, very quickly, at the root, today all the gTLDs are DNSSEC-signed. But at ccTLD level, we are still a bit below, mainly in Africa. So we only have 21 ccTLD in Africa who have signed. And when it comes to DNSSEC validation on resolver levels around the world, we are globally 28% and in Africa we are 23 or 24%, globally speaking, in terms of DNSSEC validation at the resolvers' level. So we still have a lot of work to do. And the end user community is an important partner to actually achieve this level.

So let us now come to the first poll of this presentation, just to make this session interactive. And I will request the support of staff to actually launch the polls. And also, I will hand over to my colleague, Paul, to take over from here. Paul, over to you. And staff, please launch the poll. Thank you.

Oh. Sorry. I think there was a mistake. So let us jump to the second poll. I think we forgot to launch the first poll, unfortunately. Sorry about that, staff. So you can directly go to the poll two. Thank you very much. Paul, over to you.

DEVAN REED: All right. And, Yazid, would you like me read the poll out loud?

YAZID AKANHO: Yes. Read the poll.

PAUL MUCHENE: Thank you, Yazid.

UNIDENTIFIED FEMALE: It's 22:00.

PAUL MUCHENE: Okay.

DEVAN REED: The poll question was, "Which DNS encryption techniques do you know about? Option A was DoB and DoC. Option B was DoT and DoV. Option C was DoH and DoT. And option D was none of the above.

PAUL MUCHENE: We could give around 15 seconds to complete the poll. 10 more seconds.

DEVAN REED: All right. We have 19 responses—now, 20 responses—out of 33, which sounds like a good amount. Did you want to give it a little more time?

PAUL MUCHENE: I think we can actually proceed. Maybe we want to read the responses.

DEVAN REED: All right. And I'm sharing the responses now.

PAUL MUCHENE: Okay. So for those who have answered, 55% said none of the above. 25% said DoH and DoT. 20% stated DoT and DoV. And the correct answer is DoH and DoT. I'm going to actually talk about it in the next presentation. Yazid, go to the next slide.

Okay. Yazid has talked about two aspects of DNS data security. He talked about, mainly, data integrity and how DNSSEC actually helps in enforcing integrity. And at the same time, he talked about techniques for availability, such as using redundancy and also Anycast. So I'm going to tackle the issue of confidentiality.

As Yazid has actually stated—and I share also the same sentiment—that the DNS was not actually, initially, designed with security in mind. So what we are actually seeing is that over the years, from the time the

protocol was specified in 1983 until now, we have been having, actually, security incremented over time. So you had measures such as confidentiality that was recently, actually, implemented in the DNS.

And one of these, before we talk of the two technologies that are predominately—that have been standardized—that are now being used in the DNS to actually protect data from a third party from eavesdropping, what I'd like to just mention is basically, we think, as ICANN, that data privacy is good for end users and that encrypting the DNS actually is imperative, as it protects the sender and the responder—that's the stub and the resolver itself—from on-path attacks and even off-path attacks, such as man-in-the middle attacks—even actively injecting false DNS queries, or can I say false response, between the end user and also the resolver.

However, encryption does have some major technical or policy implications. We will not cover them because of the time limit of this presentation. However, if the AFRALO community is interested, we could have a separate webinar, talking purely about DNS privacy, and also the technical, and also policy implications of privacy technologies.

The main privacy technologies we will talk about DoT, which is DNS over TLS, and DoH, which is DNS over HTTPS. But before I talk about them, I just want to mention that DNS encryption, at this stage, happens between the end user device, known as the stub, and the software at the network operator's premises, known as the resolver. This is where our discussion is going to be based upon. So just go to the next slide, Yazid.

Currently, there are two standardized protocols. One is DNS over TLS, known as DoT. And it was actually specified in two documents, RFC 7858 and RFC 8094, which is basically DNS using datagrams. It's called DNS over datagram over TLS, which is actually similar to DoT. They both implement TLS, which is Transport Layer Security. The other protocol is DNS over HTTPS, known as RFC 8484, which is actually being implemented and has also caused a bit of controversy. And the other one that has not been standardized but has been used by, especially, many implementations—especially in VPNs—is DNSCrypt.

There's quite a lot of overlap between these two technologies. But one of the key differences is that DNS over HTTPS intermingles or mingles web traffic with DNS queries. So what happens is you are actually sending encrypted queries between your device and resolver that actually has an encrypted channel that is served over port 443, unlike DoT, which basically uses a different port but the same concept. But this time, the encrypted channel is over port 853. Next slide.

So as much as these two technologies give end users the ability to hide or mask their DNS queries from a prying third party or maybe even a corporate or even a state entity, our position at ICANN is basically, we know that, first and foremost, that filtering of DNS may be beneficial.

And when we talk of filtering, we are distinguishing this from censorship. When we talk of filtering, we are talking about network operations of service-level agreements, whereby the network operator may want to maybe filter certain traffic that could be malicious. Maybe it has malware. Maybe it has spam. So in such cases, there could be a

need to actually distinguish and discriminate certain traffic that could be harmful to end users, such as malware and spam.

We also have the position that privacy is good, basically, for the end users. We actually advocate for privacy. The other thing is that we believe that DNS data should be protected. Although DNS over HTTPS and DNS over TLS, they do provide confidentiality—they hide DNS queries from an attacker or another entity—we think that when it comes to data integrity, the implementation of DNSSEC takes even higher prominence because DNSSEC helps to protect the integrity of DNS data.

And we also think that, at the same time, applications and operating systems sometimes have insufficient information to make networking decisions. At this point, it is better that when implementing these technologies, such as DoT and DoH, you should take these considerations into account. For a complete description of our position and also the characteristics of DNS [handover] on DoH, you could actually check out OCTO003, which is on the Internet policy implications of encrypted DNS. Next slide.

Currently, when it comes to the implementation of DNS over HTTPS, in the industry, Mozilla has partnered with Cloudflare to provide DoH. And it has actually enabled and option in the Firefox browsers where you can actually, as a user, enable DoH, such that now you can be able to send DNS queries, comingled also with the web queries. And Google, through their public DNS service, 8.8.8.8, do support DoH. And at the same time, we can activate it on the Chrome browser. So these are the current status of DoH.

But what about the root zone? It's very interesting but the root zone operators are not comfortable about being the early adopters of DNS encryption. They do have some concerns about DNS encryption. Since the root servers play a very critical role in the global DNS and they are often a target of DDOS, the root server operators actually issued a statement on DNS encryption. It can actually be found on the root-servers.org server, on this link that is there. And also, the slides have also been shared so you should be able to actually access the link when you open the slides.

But on the other hand, instead of DNS over HTTPS and encrypted DNS, root server operators encourage deployment of a technology known as QNMAE minimization and aggressive DNSSEC caching. I'll talk briefly about this in the next slide. Next slide, Yazid.

QNAME minimization is another privacy-saving feature and also helps to minimize exposure of DNS queries. So basically, QNAME minimization is you are actually sending just as little information as possible from the recursive resolvers to the authoritative name servers. This is actually one way of improving privacy. It's actually specified in a document known as RFC 7816.

Aggressive DNSSEC caching is basically you are querying only responses that exist. So DNSSEC caching is based on an aspect of DNSSEC, a property known as NSEC. NSEC is basically known as the next secure and it's used to show whether a domain actually exists in a zone or it doesn't exist. So this technique actually caches only domain names that plausibly exist in a zone. And anyone who actually tries to send a domain name that doesn't exist to a recursive resolver, the recursive

resolver is able to resolve this immediately without actually going through the entire resolution process, such Yazid had talked about in the first slides, of the DNS.

So my final part of the presentation is going to be on the Registry Data Access Protocol, also known as RDAP. Let's go to the next slide. So RDAP is actually a protocol designed by the Internet Engineering Task Force. It is a very, very interesting protocol, in that it has been defined in 13 RFCs, from RFC 7480 to 7493. What it is, it's supposed to be a replacement for the WHOIS. The WHOIS has actually been used since the early days of the ARPANET and it has managed to query such info about who owns, maybe, an IP address block, maybe an Autonomous System Number, and a domain name.

But unlike WHOIS … Please go back to the previous slide. Just go back to the previous slide. Unlike WHOIS, there are a few characteristics. First and foremost, it provides a high degree of differentiated access. WHOIS is actually a flat access. Anyone can query and they can get any information they can. But because of the issue of privacy and people becoming more aware of this, certain times it's better to give differentiated access and also certain rights. Another thing, unlike WHOIS, RDAP supports many languages and scripts. So it does have, actually, support for universal acceptance, which WHOIS didn't have.

This is also why RDAP is actually being implemented. One, it is a much more robust protocol. It is even more secure because RDAP makes use of the HTTPS, which actually provides encryption end-to-end between web client and also web server. And at the same time, WHOIS did not have a standardized format. But RDAP allows this and so it is much

easier to play around with. One good thing with RDAP that WHOIS doesn't support, especially for developers, is that the RDAP protocol is written in JSON. You can actually use language such as React framework or JSON to be able to … Sorry about that. It's just an alert. So this suggests some of the differences between WHOIS and RDAP.

And then, this is just for your information. With regard to the security of the DNS ecosystem, this is some of the initiatives that ICANN Org is currently undertaking. Next slide. So some of the initiatives that we are working as ICANN Org is the Knowledge-Sharing and Instantiating Norms for Domain Name Security, KINDNS. This is actually a project that's supposed to give the best practices on improving on the security and resiliency of the DNS. This is similar to the MANRS project being run by ISOC but MANRS actually targets routing. But in ICANN, we are working on the DNS and KINDNS is a similar counterpart when it comes to DNS.

And the, the DNS Abuse Activity Reporting, DAAR. We are happy that within the continent, so far three ccTLDs—Kenya, Tanzania, and Malawi—are [participating] in the DAAR project. We also want to invite more ccTLDs and help more ccTLDs in the continent to join the DAAR project or initiative.

Then, there is actually the DNSTICR, which is the Domain Name Security Threat Information Collection and Reporting. This was actually a project to report and identify COVID-related domain names, or COVID-registered domain names, that have a malicious intent. This is a project that is run by my colleagues in OCTO.

And then, there is also the Identifier Technologies Health Indicators, which is basically matrices on various aspects of the

ecosystem—collecting these matrices and trying to make sense of what they actually mean.

The next one is the Domain Security Facilitation Initiative. This is actually run by Göran Marby, the CEO of ICANN. And it actually has input from security experts within the ICANN community. It's an initiative to identify threats to the entire global domain name system and how to mitigate them.

Our colleagues at DNS Engineering have the Revised IMRS Strategy, which helps to improve the resiliency of the IMRS, which is ICANN Managed Root Server Instances, or known as the L-Root.

And then finally, there's also work that we do, both in the Technical Engagement Team, in outreach, training, and capacity building to help end users, ccTLD, and even top-level domain operators to actually improve on the security posture of the DNS.

And finally … Next slide. Okay. So these are just additional resources you could check out. And the last slide. Thank you so much for your kind attention. I think this is a chance for a Q&A.

BRAM FUDZULANI: Thank you so much. I think there was a hand in the area. I don't know if it's gone. It was from whom? Abdul, I think. Abdulkarim, you had your hand up. Or was that addressed already? Okay. I'll invite, if there are questions. I know there were some questions in the chat box and I think most of them were answered. But if anyone wants to come to the mic and raise a question to our presenters, you can [inaudible]. It looks like

… Okay. Enoch, you have your hand up. Please go ahead. Enoch, you can go ahead and ask.

ENOCH NIKINGBOUNG DUUT: [Inaudible].

BRAM FUDZULANI: Enoch, if you are speaking, we can barely hear what you're saying.

ENOCH NIKINGBOUNG DUUT: [Inaudible].

BRAM FUDZULANI: Enoch, maybe you should come closer to your mic so we can hear your voice.

ENOCH NIKINGBOUNG DUUT: [Inaudible].

BRAM FUDZULANI: No. We can't. You're not audible enough. Maybe, are you able to type? Okay. Yes.

CLAUDIA RUIZ: Hi, Bram. We also have a question in the chat, if you can read it, but it's in French. We actually have two questions in the chat—one from Olévié and another from Gabriel Bombambo.

BRAM FUDZULANI: Yeah. Please. You can go ahead and read them or anyone who can read them out for us.

CLAUDIA RUIZ: I'll read the one from Olévié. It says, "When will RDAP definitely replace WHOIS?"

PAUL MUCHENE: Okay, Olévié. I think I can take that one. What has happened is the engineers of IETF have developed a way to replace WHOIS—an alternative to WHOIS. There are certain registries—especially, I think, right now, when it comes to gTLDs, because they have contractual obligations with ICANN—they have to implement RDAP query service. So for most gTLDs, they actually have or are in the process of implementing that.

However, when it comes to ccTLDs, this may take a bit of time because ccTLDs have their own policies and practices on implementing, maybe, certain services—requiring services. So it will actual be gradual. I cannot give a definite timeline. But I think it will be quite gradual, going into the future.

YAZID AKANHO: Okay. I will take the second question, which was asked in French. So should I answer in French or in English?

CLAUDIA RUIZ: If you can please read the question in English so the interpreters can translate it. Thank you.

YAZID AKANHO: So the question is actually asking if asymmetric cryptography is the only one used in securing the DNS. And I just maybe need to clarify that Gabriel is probably talking about DNNSEC. And I would just like to remind that DNSSEC is not actually … DNSSEC is just signing the data. So we are not encrypting the data with DNSSEC. We are just signing when it comes to DNSSEC. And yes. To sign, we need asymmetric protocol. So probably key cryptography is used to sign the data in DNSSEC.

But now, when it comes to privacy—so encryption between the stub resolver and the recursive resolver—like Paul said, we are using two techniques there—HTTPS, which is based on SSL, and TLS for DoT. I hope that answers the question.

BRAM FUDZULANI: Edmond, you have your hand up. Please go ahead.

EDMOND KUNGWALO: Yeah. I wanted to understand on DNS filtering. With the issue of user privacy, don't you think that the DNS filtering will require examining the user traffic in a way affecting user privacy?

PAUL MUCHENE: Edmond, thank you. Let me take a shot on that question. Yes. One of the problems—in fact, I didn't go into this because of time constraints—with DoH and also with DoT is they make it harder for a network operator to actually conduct filtering of maybe certain traffic that could malicious. So it has been known that with DoH, maybe an attacker can send encrypted DNS queries that have malicious properties, like a command and control, over an encrypted channel. This is actually a problem.

We've noted this in the document, OCTO003. We take note of it, that as much as these technologies do provide end users with privacy, at the same time, they create new problems for entities such as network operators. It makes it harder for them to do their job. This is a downside with actually implementing these privacy technologies. I hope that answers your question.

EDMOND KUNGWALO: Yes. It does. Yes.

BRAM FUDZULANI: Perfect. Lawrence, you had your hand up but I think now it's gone down. I don't know if your question was addressed or your concern was addressed.

LAWRENCE OLAWALE-ROBERTS: Thank you. My question was in line with DNSSEC and the data that was presented with regards to adoption by ccTLDs. And my question was to find out what the peculiar challenges to adoption could be. In some quarters, it's believed that there is a level of technicality involved in maintaining the zones to keep them signed. Is that also true?

YAZID AKANHO: Okay. Thank you, Lawrence. Yes. As any other security mechanisms that you want to deploy in your infrastructure, it actually requires or requests some new experience or new competence to actually make sure that you can maintain, on daily basis, the new system. And DNSSEC is the same.

Like I said before, DNSSEC actually uses some keys, public-key cryptography. So you have to generate those keys. You have to sign the zone. You have to ensure that your signatures actually do not expire before you generate the new signatures, etc.

So yes. There are some technical challenges but this is actually why the Technical Engagement Team of ICANN has been increased—to provide more trainings and more hands-on to the community—whether it is the technical community, or it is even some government, and even the end user community, to actually provide the skills to maintain the infrastructure. So yes, it requires. But the mechanisms exist to actually get this knowledge.

BRAM FUDZULANI: All right. I think Enoch, who was not able to come on the mic, sent a question in the chat box. He says he wants to know about encryption threats and backdoors used by government, and security authorities, and sometimes cybercriminals to access encrypted data without the knowledge of the sender or receiver. I don't know whether—

PAUL MUCHENE: Thanks, Enoch. I will actually answer that question. Yazid made a presentation and said that DNSSEC doesn't … There's certain security problems DNSSEC doesn't address. One of them is the issue of confidentiality.

So when it comes to maybe a rogue government or security authorities, when you are sending DNSSEC queries between your device and perhaps the resolver, the government in question, or the security authorities, or even any other entity can still be able to see those queries and also the responses they're going to get. So in that case, DNSSEC doesn't provide confidentiality. If you wanted to provide confidentiality, you may need to use, maybe, the technologies, such as DoH or DoT.

But the other question you've asked is, "Is it vulnerable to encryption threats?" This depends on the algorithmic implementation when you're signing a zone. So when you're signing a zone, you're actually going to implement a given algorithm. It's been noticed that there are certain algorithms, even though they were standardized at the time DNSSEC was published around 2005. Those algorithms are no longer secure.

One of them is actually RSA that uses SHA1, which is secure hash algorithm one. SHA1 was actually broken by an academic—her name is Wang—in 2004. So in such a case, if the algorithmic implementation is weak, then you are actually vulnerable to [handing] out the keys that were actually used to sign your zone.

So what is recommended right now is to use to algorithms. Actually, one is called RSA SHA265, known as algorithm eight. That one is elliptic-curve cryptography. This is algorithm 13. And many zone operators, including ccTLDs, we've actually noticed, are actually using algorithm 13 and eight. Those are the most common ones because they provide a far higher degree or security and [inaudible] algorithms.

So in this case, DNSSEC still doesn't address issues such as confidentiality. Therefore, if you have an entity that wants to know the kind of queries that you're sending, it's still possible.

Your other question is what happens if a cybercriminal accesses that encrypted data. This is how DNSSEC comes in very handy. DNSSEC helps to protect against spoofing of data. I'll give you an example. So an attacker decides to hack into, maybe, the zone—a ccTLD, or a TLD, or even second-level or third-level zone operator. They access the zone file and then they actually manipulate those records. Let's assume, for this purpose, that the zone operator did due diligence with respect to DNSSEC. They decided to sign that zone but the attacker still got access to the servers.

So what will happen is this. The attacker maybe changes the zone files, changes the IP addresses. This is what happens when somebody, let's say, queries the zone. Let's say it the zone for bank.com, which is a bank.

Bank.com has legitimate IP addresses but the attacker changes them. But because bank.com was signed, a resolver that is doing validation will be able to check the signatures of bank.com. It will check the signatures before. Usually, it checks the signatures that are correspondent to the time which it was signed. And then, it checks now the data that the attacker has already modified. And then, it actually compares the results and it actually will throw an error.

TIJANI BEN JEMAA: Paul, may I interrupt you for a few seconds? We already used our 60 minutes and we are four minutes over the 60 minutes. So I would like to ask if the staff people can extend it by a few minutes so that we can answer all the questions because I am seeing other questions come in. Back to you, Paul.

PAUL MUCHENE: Okay. Thank you, Tijani. Basically, what happens is DNSSEC validation will check that the attacker has modified the data. And therefore, any queries to bank.com will be rejected. It will throw an error when you try to go to bank.com. So that's how it prevents someone from actually redirecting you to maybe an attacker's infrastructure. So in that case, DNSSEC helps in actually preventing the spoofing of DNS data. I hope that answers your question.

BRAM FUDZULANI: Okay. I think most of the … Before I pass it on to Tijani to wind up, I've seen most of the questions in the chat box have been answered or responded to unless there's any specific questions that need to be

followed up or if someone wants to follow up with a different question altogether. If there are no further questions, I would like to hand over to Tijani so that he can then give us the final remarks. Thank you. Tijani, you have the floor.

TIJANI BEN JEMAA: Thank you very much, Bram, and thank you to our two wonderful speakers. I am really proud of our young African people who joined ICANN, especially in the technical field—either if it is in the CTO office or elsewhere. But this is very important because they have to have very precise knowledge and very high-level knowledge. And also, they have to have a lot of energy because working with ICANN needs a lot of energy.

So thank you very much. We are proud of you and we thank you very much to be available every time we ask for you—both of you. I asked Yazid but Paul volunteered and I'd like to thank him very much because he volunteered. So I would say that this has been more than we are expecting. So thank you very much, both of you. I think that it was very useful for our community.

I would like to tell you that we have one remaining webinar for this year. It will be in November, normally. I hope we will be able to hold it because there is a lot of events in November but we'll try to do it.

I'd like to thank our staff, the interpreters, and all of you who came here. The webinar was to give you more information and more knowledge to be able to participate and to contribute in the statement drafting. So please volunteer and go and draft the statement. This is the only way to

learn how to draft a statement, how to draft an opinion, how to raise the voice of Africa. So thank you very much, again, to all of you. And this webinar is adjourned. Thank you. Bye-bye.

DEVAN REED: Thank you, everyone. Have a wonderful rest of your day.

TIJANI BEN JEMAA: Thank you. Bye-bye.

SILVIA VIVANCO: Thank you very much, everyone. Bye-bye.

[END OF TRANSCRIPT]