KOBE – SSAC Public Meeting
Wednesday, March 13, 2019 – 15:45 to 16:45 JST
ICANN64 | Kobe, Japan

ROD RASMUSSEN: All right. Hello, everybody. This is the public SSAC meeting. We're going to get underway. And Jay, come on up here. Thank you.

I'm Rod Rasmussen, SSAC Chair. Julie Hammer, SSAC Vice-Chair to my left. I think, when looking around the room here, most of you know us but it's good to see friendly faces. And I see a few new faces too, I think. So hopefully, we'll get a few more people coming in.

I'm going to go over what the SSAC is for those who are new to our work and talk a little bit about how we do our processes. And then we're going to talk about some of our current work. I'm going to give an overview of our current work, some of our future work, and we're going to do deep dives on several different topics and then have room at the end for questions. I will pause after some of the major topic areas to take audience questions for a minute or two depending on if there's interest and we'll try and keep it moving along so we cover all our topics today.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

Okay. So here's the agenda. I could have put that up here while I was saying that. So these are the topics we're going to be covering today.

So SSAC, Security and Stability Advisory Committee, we are currently 39 members and that's a size that we've been approximately for a while and it goes up and down a little bit around that. But we have a unique role in directly advising the Board on SSR issues: stability, security and resiliency issues affecting the DNS, and in particular, the naming systems.

We also have a broader responsibility to the overall ICANN community to bring issues to various parts of the community, especially when there may be things like a new attack or something that might affect a significant portion of the community and also try to do our best to bring current and emerging issues to the fore.

We have published over 104 publications and many other communications over the years and we have a wide variety of expertise. One of our goals is to have diversity of technical capability and security experience so that those of us who have knowledge in one area can be supportive and help other knowledge that other experts bring so that we can look at problems in their entirety. And you can see a list there of all the different kinds of things we focus on.

So the unique role we have is actually tying right to ICANN's mission around the stability and security of the naming systems. And in that role, we try and focus our work in those areas. And we do talk to broader security topics as well, but with a focus typically on the areas that will affect the ICANN world as it were.

The way we work is to form work parties, so as you can see, we don't have all 39 of our members here but we have a good portion here and what we do is we'll form a group of people who have expertise or interest in a particular subject area that we're dealing with.

We will research and work with our very helpful staff on writing things up and bringing in, and sometimes we'll even bring in outside experts to be part of that work party. But we typically work internally and then that work party will provide that report.

They will finalize what that will look like and then the entire SSAC then reviews that as a whole, may send it back to the work party for further work, may decide that this is something we don't want to talk about.

But eventually, if we publish something, it will have the full consensus of the SSAC. But we do, of course, on some issues, we'll have differences of opinion about items. So we allow for dissents as well to be published. We look at that as being important because there are multiple sides to issues, especially speculative issues, so if you see some dissent in an SSAC document, that's us trying to be transparent about the issues and bring the full set of possibilities.

We do have that unique role I mentioned to the Board where our advice goes to the Board and that actually kicks off a process where we make sure that they understand what we meant and we'll clarify things as needed to make sure that we are all on the same page.

And then they'll take some sort of formal action if we have recommendations that require it. That action will typically be some sort of resolution that could feed into various things. It could be something [takes] that policy. It could be something that actually creates a job for ICANN Org to build a system or something like that. There's a lot of different things.

We have, since our last meeting in Barcelona, we have put out three of our primary documents. We also have several other of our correspondence series, which are more administrative in nature, that we've put out as well. We did an update to SSAC 101 which was published in the middle of last year. That was part of that clarification process that happens sometimes when you have to take a look at things and update them to make sure things are clear. But we'll get into that in a minute.

We had our response to the SubPro Initial Report and some comments on the work of the EPDP that was going on in December. Obviously, events have moved along rapidly after that, but a lot of those comments still stretch, or still stand looking forward to Phase Two and we'll talk about that a little bit more.

We have the Name Collision Analysis Project. We have a section on that we'll talk about in general. Our Organization Review is still underway. That is kind of in its implementation phase to some extent. Well, it's in the phase where we're going through the final report and providing our response back and then there's some more work that gets done after that but this is kind of the wind down where we're taking on all the suggestions and commenting or implementing them internally ourselves.

We have work we're doing on the Internet of Things. That's what IoT stands for if you haven't heard of it before. And we're going to have a bit on that in this presentation as well.

We're doing some work on our own internal working processes. This is in conjunction with things we've gotten back from the Organizational Review and things we decided on our own in our own internal revealing.

We have an engagement with regular basis at Tech Day which was on Monday where we talk about emerging security topics.

This past Monday, we talked about domain registration hijacking and some of the things going on there. DNSSEC Workshop, which was today, is related SSAC as well. Although that largely stands on its own.

We have a membership committee. We are always looking for new qualified members and we have a process where we take a look at the skills that the members could bring, or a potential candidate could bring. Sometimes we don't accept qualified people, not because of anything other than we already have plenty of qualifications in that particular topic area and we're trying to diversify our technical skills.

Speaking of that, we also are always looking to diversify our make-up on the more traditional ICANN types of diversity goals and we have a particular interest in diversity in geographies where network infrastructures are not the same as the large established Western large scale networks. We're always looking for people who have to deal with security issues in a much more challenging environment and looking for that kind of experience. So if you know a very well-established security expert, networking expert, etc. who can bring that kind of experience, we highly encourage you to ask them to apply. The application information is on the website and as I said, there is a process that has to be gone through but we are always looking for qualified folks that we can bring in and diversify our skills.

The other thing that we have, we finished off some joint work with the ccNSO on the EPSRP which has to do with some [string] similarity things. In particular, there were some issues around dot-EU in Greek that were kind of driving that and that, the ccNSO has issued a letter on that. We put this here mostly for Göran, I think, because he's been bugging me about it for quite a while and it's done.

Possible new work. We're looking at the various, I'm calling them the Killer Ds right now. We have these acronyms, DoH, which is DNS over HTTPS, DoT, DNS over TLS, and DPRIV, DNS Privacy. We also have DoC, DNS over the Cloud. There's a whole bunch of other things that all start with a D for DNS.

And this has to do with encryption of DNS, typically in transport methods for that but also how it's operationalized and we're hopefully about to kick off a work party on that. There's a lot of questions on that.

So other things that are potential work topics. Looking at hyperlocal route, this is something that we may do in conjunction with RSSAC, the Root Server Security Advisory Committee. We also have a few issues around DNS key management where there may be multiple parties involved in the management of your DNS and/or changes of control when you're moving from one provider to another and how that plays with DNSSEC.

We have an open item discussing handling techniques, best practices around takedowns. Obviously, in this context in domain names, when and how, and etc. how that might be appropriate or not.

Looking at particular issues that we're seeing in the data around abuse of the new TLD program, hopefully this will inform subsequent work, or subsequent rounds, lessons learned and things like that. We'd like to be able to provide some information then there. Then looking at recent series of domain hijacking attacks which have very high profile targets and fairly sophisticated understanding of how the DNS system works, so we'll have some more on that in the presentation as well.

So before I hand that over to Greg Aaron to talk about SSAC 101 version 2, were there any questions on any of the topics that we may be doing or the topics we're currently working on?

Okay. Greg, I'm going to turn that over to you. You want the clicker? Okay.

GREG AARON: Thank you. SSAC 101 was first published back around the Panama meeting last summer and then we did an update. We're mentioning it especially here because it has some recommendations and some background in it that are relative to the EPDP.

In general, this paper was about how do you get access to data? What is it used for? What are the impediments to it? And what are recommendations about it? Basically, the issue was twofold. One is WHOIS data is no longer accessible for legal reasons in many cases, the GDPR being the main driver of a reduction in the amount of contact data, especially, that is available. And we talked about some of the legitimate interests that security practitioners have and how they use that data.

The other topic of this paper was about rate limiting. This is when a party is limited in the amount of information they can get from the system or the frequency and some of the issues around that because timely access is also really important for protecting people and networks. So we will continue to rely on the advice given in this paper as the EPDP continues.

One of the things that the EPDP Phase 2 is going to be looking at is an accredited access program, which is something that the SSAC has supported and we'll talk a little bit about that later.

ROD RASMUSSEN: Okay. Thanks, Greg. Were there any questions on SSAC 101v2?

Okay, good. I'm going to pass that over now to Ben Butler to talk about what's going on with our involvement with the EPDP.

BEN BUTLER: Thank you very much. The SSAC has been involved in the EPDP from the start with very high hopes, but I would call it also with a fairly clearly defined and narrow focus. We wanted to make sure that we were focusing on issues as we go through the EPDP process that would have security and stability implications.

There's a lot of things that are important and critical policy issues wrapped up in that, but our expertise is in the security and stability. So to that level or to that point … Is this SAC 104? Is this one of yours? Okay. Sorry, we had some slide confusion there.

So in the final report that was published from the EPDP for Phase 1, there were a few things that we wanted to call out that SSAC generally had joint consensus on nearly all of the recommendations. We had two dissenting opinions and I wanted to clarify a little bit about what those were.

There was also one where we joined the consensus but with a clarifying comment as to the urgency that Phase 2 needed to commence its work. The access question that everyone loves to dream about and no one loves to hear about is something that we really feel needs to be happening with as much urgency as possible. So that was one of our clarifications.

We also then made some clarifications about WHOIS accuracy and among all these discussions, there has been a little bit of loss of perspective about an important security and stability function within the ecosystem where security practitioners and general Internet users who come across a malicious domain name have the ability to report invalid WHOIS data and that was actually an instrumental tool in getting a lot of malicious domain names taken down in the old regime, and that is now largely impossible under the Temporary Specification.

So we wanted to make sure that there was mention that accuracy and a third party reporting mechanism needs to exist in the new regime as well. We also made some clarifying comments about particular data elements that we wanted to make sure stayed around as far as support, specifically, the ability for a registrant to specify a technical contact for a domain name. There are legal and policy questions wrapped up in that and those are going to be discussed in more detail in Phase 2 but we just wanted to call out that we think that is a critical thing for there to be support for from the registrars and registries.

In our dissentions, realistically, the dissentions were based in a particular detail and not in spirit. Recommendation in 16 and 17 respectively were both recommend that registries and registrars should have the option to attempt to differentiate both on a geographic basis and a legal versus natural persons basis. We think that those are very worthwhile activities but we think that it should be a requirement, not necessarily an option. So those were the formal dissentions that we lodged in the report. There are other groups within ICANN that support this and is something that we will be discussing again as we continue in Phase 2.

I always feel like I'm kind of rehashing the same points, but as we move forward into Phase 2, there are a couple of things that we, as SSAC, are very kind of focused on and we want to make sure are discussed. We don't yet know all of how that will take form, but obviously, some of those things will include what data elements cyber security practitioners need and how we can best facilitate them being able to access that data while still being compliant with GDPR and the data minimization standards.

We are going to have to spend some time thinking about it and helping flesh out the parameters about accreditation for security practitioners. To be clear, that is not SSAC saying we are going to be the accrediting body by any means. We definitely don't want to do that, but we do want to make sure that that is a parallel process that's happening so that when an access system is created, there's not a bunch of security practitioners with no way to accredit themselves. That would be a bad solution. And we want to look at things like correlation of pseudo-anonymized data so that bad actors and domain names belonging to them could be identified in some way.

And as a clarification, that is not to say we are trying to create the stigmatic reverse WHOIS, but that we believe there are ways we can facilitate correlation of non-personal data in a way that would be meaningful for security practitioners, and just making sure that the ecosystem in general, the DNS ecosystem, is part of the balancing equation in all that we continue to discuss in the EPDP.

The privacy rights of individuals are clearly important. The rights, responsibilities and risks of the contracted parties are important, but also, the possible risks to the ecosystem if security cannot continue as it should in the Phase 2 solution.

Any questions about our involvement, our participation or anything that you would like to see us make sure we're thinking about as we go into Phase 2?

ROD RASMUSSEN: Can we get the mic on, please?

TIM CHEN: Let me know if I need to do something. There it is. Tim Chen with DomainTools. Just two questions on this section. One is, and I think you were alluding to this, Ben, but looking forward, I think it's going to be really important to have a very specific idea of how security practitioners, how you define what that is and how they get credentialed. Just looking at the staff on law enforcement to kind of rights holders, something very tangible in each case to hold onto as you go throughout credentialing our approval process for access.

And as I'm sure you know, security practitioner is somewhat undefined. Before you try and define it, I think that's something hat's going to be heavily debated and getting ahead of that, I think will be helpful.

And the other thing just crossed my mind is the invocation of GDPR and the law is so heavy in this whole process and a lot of the organizations that are involved, either themselves or attorneys or they have paid legal advice – I don't know where this falls in SSAC's budget – but even I think wading into ideas like, "Hey, we should do a balancing test that includes the harm to the public interest," which I totally agree with. I can almost predict pushback as if that's irrelevant, legal concept to introduce in the process. So maybe think about whether or not you feel like SSAC needs some legal advice for your own debates to make your feedback either more powerful or more approachable to the process. Thank you.

ROD RASMUSSEN: Thanks, Tim. We appreciate the inputs there. This is the first time, I think, I've ever heard somebody suggest SSAC hire a lawyer, hopefully. I take your point, though. Actually, I'm going to use that as an opportunity to point out that I think the SSAC, as part of SAC 104, highly encouraged ICANN Org to support using legal counsel in support of the EPDP and we certainly see that that was helpful and would be very helpful going forward. That advice stands, as we like to say, and just support in general around that for …

Some of those questions you were bringing up around how do you define these things, there may be a role for SSAC to help in that area so we'll take that one on as an area for us to take a look at. There is work going on as I'm sure you're aware, but others in the room may not be aware, around some groups like MAAWG and the Anti-Phishing Working Group and others that are looking at how they might do accreditation programs for security professionals, and definitions are part of that.

I think one of the keys there is norms and how they are actually, the way they're going to behave is the drivers rather than necessarily some other things. Anything to add, Ben?

BEN BUTLER: The only thing I would add, and I completely agree. I love it when Rod and I have very similar thoughts. We definitely are in support of continued use of independent legal counsel and we want to make sure that we, as SSAC, are putting questions like that into the process. Or I should say we're putting issues like the risks the ecosystem into the questions that get sent to the legal advisor so that that balanced test can be done.

I would also just add that on Rod's earlier comment that we are always looking for ways to diversify the talent that we have within SSAC. I have to use this as an opportunity to thank the other members of the SSAC EPDP Working Party. Benedict and I are actually participating every meeting, but we can only do so because of the support and we have a broad range of folks on SSAC with varying and some very impressive amounts of legal and policy experience, not just the Internet tech nerds. Though we have those in abundance as well.

So I'm comfortable representing SSAC on this effort because I know we do have that diverse skill set.

ROD RASMUSSEN: Okay. Thanks, Ben and everybody, and thanks for your question. Tim April is going to run through an area where we have actually a lot of concern as SSAC and we're taking a look at potential new work. Tim?

TIMOTHY APRIL: So as many people probably already know, there was a recent large scale attack on domain registrations where many registration records in ccTLDs and some TLDs were hijacked and used to attack the end user, the owners of the domains and some of their users. The attackers were modifying DS records and re-delegating some of the zones to different name servers and then they were intercepting traffic using man in the middle proxies, mostly through the use of compromised credentials.

The advice that we're giving right now, or the suggestions we're giving right now is that anyone who is either a registrant, registry or registrar, so most of the people within the ICANN community, should be taking a look at the security of their system.

So there's no Holy Grail, there's no silver bullet to protecting yourself, so securing your credentials that you use to contact your registry, registrar or service providers, whatever, strong passwords, no [password] use, enable MFA where possible. If you don't have the option to use MFA, ask your provider so hopefully they can enable it.

[ROD RASMUSSEN]: What is MFA?

TIMOTHY APRIL: Sorry. MFA is Multi-Factor Authentication, sometimes also known as Two-Factor Authentication or Two-Factor is a subset of MFA.

And then the e-mail address is used for domain registrations, so things that may appear in the WHOIS records, those should be also looked at too because they can be often used for password reset notifications to further compromise domain registrations.

And then signing and validating DNSSEC could reduce some of the impact of this type of attack, but it also will not fully prevent it. And if your registry allows domain locks and your registrar does, consider enabling domain locks and then monitor your domain infrastructure. There were at least two other sessions this week that cover most of this that you can find on the ICANN website.

And then, finally, this is not the first time we've seen this type of attack but it sure won't be the last. So be on the lookout.

If you'd like to refer to some of our past publications going back as far as SAC 40, there is a whole bunch of data or information about how to help protect your domains.

ROD RASMUSSEN: Thank you, Tim. There was a session this morning where there was a lot more in-depth on some of the information of the attack where Tim and [Medica] and Danny McPherson who is not on stage currently, but three SSAC members were part of that and it was a very good session. So hopefully, you were able to attend that.

Were there any questions on the domain hijackings bit right now? Or we'll go on to the end cap stuff. Okay, good. Nope, we got one. We got Bruce. Come on up.

[BRUCE TONKIN]: Yeah, probably more just an additional comment. I noticed on your slide, you had a number of precautions that registrants should take, including more multi-factor authentication, etc.

One of the things I've noticed also, though, is that people aren't clear when they register domain names, who is actually legally the owner of that name or the holder of that name because, quite often, people get their web developers and other people to register their name for them as part of developing a website and they often will register the name using their own identity, if you like, the identity of the web developer. And then that web developer disappears.

And then when your name has got hijacked, you can't even prove to the registrar that you are, in fact, the rightful holder of that name and the name should be transferred back to you. So just something that you might want to consider in your advice is adding, "Make sure you know who is the correct legal holder of your domain name as recorded by the registrar."

ROD RASMUSSEN: Excellent point, Bruce. And I think we may have covered that in one of those publications back from the day. In 74? Okay, very good.

And that actually ties into kind of more of an older school problem around domains and ownership. Ironically, of course, now it's even harder to track down and prove who may have had control over the domain name. It's very difficult to have a public record of it in many cases now.

But let's move along to the Name Collision Analysis Project. There will be, just as a prelude to Jay's comments on what we're doing, there is a Board resolution outstanding for tomorrow on kicking off the first study here. So Jay, if you can get us some more details, give it to you.

JAY DALEY: So this is the thrilling part of the talk that I know most of you have come for, so thank you very much.

Name Collision Analysis Project, the snappiest title we could find for this one. So about 18 months ago, possibly a bit longer ago, the Board passed a resolution asking SSAC to conduct some studies and provide them advice. This is one of the most detailed resolutions the Board has ever passed asking SSAC for advice, went on for ages and ages of a very long resolution.

We'll start off with a – thank you – proper definition for name collision and then criteria to help the Board determine whether particular strings could end up being delegated as new gTLDs. There's some detail in there, but that's effectively it.

To give you a bit of background so you understand, there are certain strings such as dot-home, for example, which were applied for during the last round, which have not yet been delegated and where they had been used in a private context by a number of businesses and others, and as a result, there is already traffic from that private usage leaking onto the Internet and if it were to be delegated, then there are potential problems that would come from that.

And rather than just say, "It serves you right," there is actually a process going in place to understand what the impact would be and whether we can do anything about it before we then say, "It serves you right." No, I take that back.

So the studies were to be conducted in a thorough and inclusive manner, and in particular, we were asked to talk to other technical experts rather than just do them ourselves and engage widely with other people.

So we produced a project plan about this last year, which broke this down into three studies. The first one is to look at the existing work that has taken place and understand what gaps come from that existing work. The existing work was reasonably thorough, but it was some time ago and we didn't have as clear an understanding of the problems that exist as we do now, and so somebody needs to look at the results that were produced last time and give a synopsis of those. So that's part one.

Study 2 is then to work out what causes name collisions and what the impact is of those collisions, and the sizing. So to give you an example, there may be a Voice over IP system that is commonly used that uses a domain name in a private context and that may leak onto the public Internet. And if that is then delegated, that domain name, to create a top-level domain, that may then impact that Voice over IP system so it sends its calls to the wrong place. So that's what we mean by the impact.

And we may be able to work out that there are 10 million copies of that installed and so we may end up with 10 million phone calls per minute going to the wrong place, for example. So just a rough aim of Study 2.

Because, of course, if there is a particular thing that causes a collision but it is at a very low level, then that's when we can say, "That serves you right." And if it's a much, much larger one, then it would be, perhaps, less responsible for us to say that to people.

But Study 3 is then, a number of people have said, "Well, we understand there's a problem, but here's an idea how to fix it," and so what we will be aiming to do in Study 3 is get everybody's idea about how you can fix these things and see whether we can test those or find out whether anybody else has any evidence that shows that they work, so that we can end up with these mitigations for a name collision. And then, hopefully, that would mean that a string that is known to cause an issue could possibly be safely delegated at the end of that with those mitigations in place.

Right. There will be a short test on that afterwards, so I hope you're paying attention. Good.

The first meeting of this was actually on the 12th of January, 2018. Then we wrote a project plan for it which I've just explained to you. That went out to public comment. Detailed comments were made and responded to. Now I'm not going to go through all of the comments, but just briefly to say that a lot of the comments were people asking us either, "Could we please insist that the next round of new applications is held off until the end of this work?" and other people saying, "Could we please ensure that nothing stops the next round, not even this project?" And our answer to both of those was that's the Board decision, not ours.

In response to the comments and in response to some Board questions, we revised the project plan. But in doing so, we realized something quite important, that this is a huge project, it's very different from anything else that has ever been asked of SSAC and has a fixed budget, potentially in the millions. It has a fixed timetable and it makes extensive use of contractors.

And so we went back to the Board and said, "Look, this isn't really an SSAC advice type working party. This is an ICANN project to which we should be providing advice." And we asked then if ICANN Organization could run that project rather than us running it. They agreed and then OCTO, which is the bit of ICANN that looks at these things, began to work on looking at the project plan that we had produced and they came out with some minor amendments and those minor amendments are then being agreed by the Board very shortly.

So when that is all done, we hope to actually start the project. That would be quite nice. And that will mean setting up a mailing list that you can all get involved in. There will be certain rules around that and then we'll be looking particularly for external people to work with us on that project, external technical people.

So briefly, this is the management structure. The project customer is the ICANN Board. The project steering group is the Board Technical Committee, the SSAC leadership, the Name Collision Analysis Project Co-Chairs, of which that's me and Jim Galvin, and OCTO. OCTO will be the project director and owner, and then SSAC will be the project technical architect.

So any questions on that at all? Well, that's disappointing. Surely, there's one question. No, I don't mean it. Good. Right. Okay. Thank you.

ROD RASMUSSEN: Thank you, Jay. So just to put a point on this, this is going to be a fair amount of work, assuming of course, that this does pass the full Board. These things typically do when they get to this stage, so we're not anticipating any issues there.

And there are some, one of the questions we've been asked in various venues is, "How is this going to fit into Subsequent

Procedures Policy Development?" and then the kind of implementation rounds, i.e. building a new guidebook, etc. So we're looking to at least give some guidance around that. We actually did that earlier in the comments to the Subsequent Procedures, so we're aware of that and have some thoughts on how things will interweave with those other efforts that are going on. So we are well aware.

Now for our final in-depth area – sure, thanks – we have our Internet of Things Work Party which we have a paper that we did some work on here this week and is going to actually go to full SSAC review and hopefully will be published very soon and some excellent work. And Cristian has been spearheading that. And over to you, Cristian.

CRISTIAN HESSELMAN: Thank you, Rod. So this is the IoT Work Party. So as Rod already mentioned, we've produced a report which has the title "The DNS in the IoT: Opportunities, Risks, and Challenges". And in that report, we basically explore the Internet of Things, and in particular its role for the DNS.

And the Internet of Things is basically, we consider it a new type of application of the Internet which is different from traditional applications in which users interact mostly with content and services. But in this case, the IoT is basically something that consists of a large number of sensors, actuators and that sort of thing that sends and act upon the physical world. And this usually takes place without user awareness and involvement, so this means that the IoT is something that is more of a pervasive system that operates in the background of people's daily lives, if you will.

So the operating environment is much more heterogeneous than we are used to, so usually it's smaller phones and laptops that we're talking about, but this time it's all kinds of sensors with different kinds of operating systems, different actuators with different CPU architectures, different wireless connections, and all that sort of stuff.

And we know that many of these devices that we see out there currently are using the DNS to locate services on the Internet and they need these services to carry out their tasks. So we know of one example, for instance, where there's a light switch and you flip the switch using an app on your phone and the message travels through a service that sits on the Internet before it actually switches off your light at home. But there can be more advanced scenarios in which the service on the Internet analyzes sleeping patterns or that sort of thing.

So the goal of this report is actually to do two things. One is to explore the opportunities and risks, opportunities for the DNS in the IoT, in particular, to make the interaction of the IoT with the physical world, to increase its safety for end users. And the second one is to discuss the risks that the IoT may pose on the DNS.

And our second purpose is to kind of de-buzz the term IoT, and in particular, explore what it means from a DNS perspective. This is also relevant for the draft strategic plan that ICANN published a couple months ago, so that's the strategic plan for 2125 that also explicitly mentions the IoT, but let's say in the context as a risk for the DNS and the Internet.

So we ended up with a couple of challenges for the DNS industry. So based on this analysis of opportunities and risks, we identified five challenges and this is basically why, and that's different from a normal SSAC advisory so we don't provide any recommendations but we provide a number of challenges which go beyond the ICANN scope, basically. So this is also why the product that we're putting out there is a report rather than an advisory.

So the report basically has four components in there. Three of them are on this slide. The last one is on the next slide. So the first one, we discuss a model of the DNS in the Internet of Things. So how do devices interact with the physical world, with backend services and how do they interact with the DNS? Then we discuss opportunities of several DNS technologies and how they may provide an advantage, how they may increase the value of the DNS in the IoT. So one example would be DNSSEC, for instance, which would prevent that IoT devices are being re-routed or redirected to malicious backend services without users being aware of that because IoT devices may not have a user interface so users might not even be aware of the fact that their device is being redirected to a service that it's not supposed to end up at.

In terms of risks, we looked at several risks. I'm just going to pick out one. So we had a look at the size and complexity of IoT botnets, for example. We looked at several measurement studies that were published in academic papers, and from that, basically concluded, for example, that IoT botnets are growing in size and that vulnerabilities of IoT devices get exploited more quickly and that they're also likely to be more difficult to fix because IoT devices are much more heterogeneous than what we're used to in terms of laptops and mobile phones. So this poses an additional risk for DNS operators that they need to deal with.

So after this, based on these challenges and risks, we came up with a number of challenges for the DNS industry. So one of them, the first one, would be to develop a DNS security library for IoT devices. So this would mean making things like DNSSEC signature validation and DoH and DoT available on the IoT devices and so the underlying work that needs to be done is to develop this library and make it available on various operating systems for the IoT CPU architectures and that sort of stuff.

Another example would be developing a system that would enable DNS operators to automatically share information on IoT-powered DDOS attacks. For instance, in terms of the IP addresses being used, protocols and port numbers, and that sort of stuff. So that they can send this to other DNS operators who are then prepared for the attack in case it comes their way.

So the next steps are, as Rod already briefly mentioned, is to go through the internal review within the SSAC and if we get that done, we will publish the report and ask the community for feedback.

That's one too far, so that was it. Thank you.

ROD RASMUSSEN: Thanks, Cristian, and just before, if you have some questions on this or on IoT in general around the DNS, please come up to the microphone. I was going to put a little bit of a point on this particular one and the way we've approached this is that this is going to be more of an advisory and a codifying of the various risks and opportunities Cristian just outlined and not a set of recommendations at all. This is very much trying to define the space vis-à-vis ICANN and the ICANN community because there's a lot of really good work going on in many places in IoT and we don't really want to just repeat what other people are saying but actually bring those issues that are affecting community members, in particular, to the fore.

From the feedback that we may get from this, we may actually take on some recommendations and things like that to follow on, but what we'd like to be able to do is get feedback from the community in how the issues that we brought to the fore and see if there's questions or a desire for us to speak to any particular risks or particular programs like, for example, the one he mentioned here around deploying a system for informing around IoT attacks.

I see somebody coming to the microphone. Yea.

WENDY SELTZER: Well, I hear you asking for questions, and not having seen the report, it's mostly questions about whether you are addressing the questions around at what layer should the security questions and considerations be addressed. There are plenty of aspects of IoT security that are addressed elsewhere at application layer, for example, certificate checking or in software application design, such as recommending frequent updates and automatic updates as ways to mitigate security risks. Is that a part of what you plan to discuss?

CRISTIAN HESSELMAN: That's a very good question. Thank you. The answer is no because there are various documents out there. So ENISA produced a document, which is a European security organization, and there is ETSI and they produced these documents on what to, how to make requirements for IoT security and they're very generic.

This document is different in that it only focuses on the combination of DNS and the IoT. That's it, nothing else.

WENDY SELTZER: Thanks. I look forward to seeing it.

ROD RASMUSSEN: Okay, any other questions on the IoT? Okay. So now it's our turn for questions to you. This is the point where this is your chance to get up and tell us about the areas you think we're not covering that need coverage or things that we need to be weighing in on from an SSR perspective. What are some of the things that you would like to see us prioritize as work? And for that matter, the work products that I mentioned that we're considering, are there things there that you think are a really high priority that we should take into consideration?

So please come on up and bring whatever you've got. We have another six minutes and I'm going to flip it back to the potential new projects. If you're looking for a mic, you've got to go all the way round to the other. Yeah, okay. We've got a couple of folks coming up but I'm going to flip this back while you're walking up. Oh, go ahead.

[SARU]: Hello, I'm [Saru] from NextGen. And yeah, I'm starting to research about security of the IoT and overall [inaudible]. And I'm thinking about you put some layer of security using another IoT device as an [IDS] system. So [true protect] about the DNS systems attacks IoT. What do you think about it?

CRISTIAN HESSELMAN: So thank you for your question. I think that's a very good one. So if you look at those IoT-powered DDOS attacks, we believe that there is no single silver bullet that you could use to handle them. So you will need to have multiple mitigation strategies in place. So for example, at the receiving end of a DDOS attack, you will need to have scrubbing services, for example. But at the same time, you can also extend edge networks with intelligent systems that, for instance, are able to automatically detect devices that have been infected with an IoT botnet and then rate limit them or temporarily cut them off or something like that.

So if you really want to handle the IoT botnet problem, you will need to do multiple things at the same time, including enhancing edge networks with cyber security systems. Does that answer your question? Okay.

ROD RASMUSSEN: Thank you very much. Next up, please.

ELLIOTT MANN: Hi, my name is Elliott. I am NextGen from Australia. I have just more of a general question. At the beginning, you discussed the process of how SSAC works in terms of forming the working group and everything. I was just wondering about the step before that which would be issue identification. I understand earlier you mentioned issues passed to you from the ICANN Board but I was just wondering if you can self-start issues and particularly in the Asia-Pacific region where there's a lot of emerging countries and economies and everything, just wondering if there you have intelligence from particular countries that then refer directly to SSAC and you start from there as well.

ROD RASMUSSEN: Great question. I really appreciate that. I should have actually covered that a little bit better in the front. Yeah, we have a combination of ways to get work kicked off and prioritized, one of them being the Board may ask us a question like they did with end cap. We actually have studied this. It was changed over time and up and down, but we typically do things internally.

Our own members will have ideas around things they want to cover and they'll kind of get in the pool of ideas and then we'll see. Part of what we do is take a look at what the interest is, how many members are interested in covering a topic and then also, my job as Chair and our admin committee will take a look at the skills we have because if we have the same kind of topic area, a bunch of work parties going at once with staff, that means it makes it really difficult so we'll try and load balance it where our skills and our interests so that we can have our members working on different things at the same time. So there's a combination there.

On the other question, that gets into the recruiting thing that I brought up earlier. We want to get more information now. Our members go to conferences. We are parts of mailing lists. IETF and various things like FIRST, the Incident Response Security Team where you have people that are in those regions and they're participating as well. So we get that intelligence. It's best to have boots on the ground first, then intelligence.

One more question real quick, I see there, because we've got just a minute left.

VICKY RISK: Hi, Vicky Risk from ISC. I'm not sure if this is an appropriate topic for you folks, but I wish someone, maybe ICANN somehow, could provide a service that would allow a domain owner to subscribe to alerts when someone is trying to get a domain validated certificate for their domain. It seems like that would be a really useful thing.

There is such a thing? Okay, well.

UNIDENTIFIED MALE: I guess I'll try. So I mean there is certificate transparency, which you should be able to get a list of all certificates that are actually issued for a domain. But your question specifically said when people are trying to get a … Yeah, sure. So certificate transparency is a public log of all certificates that are issued and so you can subscribe to the list and watch for your specific name, or more likely, ask a service to subscribe to find a service which will give you that alert and there are a number of them which do that. But certificates only end up in the certificate transparency log after they're issued. You won't find out before a certificate gets issued. And we can chat more after.

ROD RASMUSSEN: Great. I thought you were going to go into changes to the domain name in the DNS where something like that doesn't exist. There's been some discussion around that.

We are at our time, so I would like to thank the audience very much for your great questions and the next session in here starting at 5:00 is the meeting with the technical experts group, so I'm sure that many of you will continue on for that. So thank you very much.

[END OF TRANSCRIPTION]