ICANN Transcription – Abu Dhabi
GNSO – Non Commercial Stakeholder Group (NCSG) Open Meeting Part 2
Tuesday, 31 October 2017 17:00 GST

On page: https://gnso.icann.org/en/group-activities/calendar

Roy Arends: So my name is Roy Arends. I work for the Office of the CTO as a researcher. This presentation is about (unintelligible) to delay the KSK role, was supposed to happen on 11 of October. A little bit of background, when you do the DNS SEC signing, when you do DNS SEC signing and validate DNS SEC records, you need a trust anchor. And the trust anchor is a public key and cryptographic (hygiene) such that public key should not be forever. And this trust anchor should probably be periodically renewed or in DNS SEC terms we call it rolling.

You can do this automatically or manually. And about seven years ago, we wrote our DPS, the DNS SEC policy statement where we had an agreement with the community that we do this after five years. We're now after five years.

Excuse me. When you roll trust anchors it means that your validator needs the new trust anchor. There are various ways of doing this, a popular way is RFC 50-11 which is basically automatic updates to the trust anchor. You can do this manually or you can have some other automated update mechanism.

However, for us at ICANN, there's no way to know which keys you have configured.

And we knew this, so we had a multiyear design and outreach effort, we had a design team and we had ROCs, we did outreach presentation various venues, various plans. We talked to vendors, we talked to governments were contacted etcetera, etcetera, just to make them aware on that on the 11th of October, 2017, we would roll the key.

Now rolling the key takes a significant amount of process and so in July – excuse me – in July 2017 on the 11th, we introduced new KSK. We can actually see on root server traffic if there are any problems, the resolvers will get very aggressive and if there's a problem and they will ask for the DNS key very aggressively. That didn't happen so we continued.

And on the 10th of October, 10th of August, excuse me, the 30-day hold down timer ended and the 30-day hold down timer is a specific element in RFC 50-11 that requires a validator to observe the key for at least 30 days before configuring the trust anchor.

And then 19 September, this is where VeriSign, our root zone management partner, do their regular – their every three months as (unintelligible) rollover. They have been doing this for – since 2010. There's nothing special about that except that on 19th of September the key size was bigger than it ever was before.

Again, we didn't see any problems, so we didn't feel the need to fall back. So I have the timeline here. Excuse me.

Milton Mueller: Excuse me just for clarity, when you say the size of the response you mean the time, the duration of the response or the – what do you mean by the size?

Roy Arends: The size literally the amount of bytes in the UDP message.

Milton Mueller: Okay.

Roy Arends: You can see those times on the graph that I show you here. The middle line is July 11 where KSK 2017 was published. The green that you see here are resolvers that signal if they have KSK 2010 and KSK 2017. And the red that you see here are resolvers that only have KSK 2010. So in this sense green is good; red is not good. You see this beautiful swap a few days later on August the 10th where resolvers basically start using this new KSK as well – or sorry – configure the new KSK as well.

And you may ask yourself how do we get this data? Well I just said, there is no data available, it turns out there is an RFC, and we knew this, excuse me, sorry, I don't know what is going on. We have an RFC 8145 that allows a validator to signal the trust anchors that they have. But it was so new, it started in April 2017, it published in April 2017.

And so we only got a handful of signals and before we actually dismissed the data because it was so incredibly little we had no idea what to do with it, it's a representative sample. At that time we only had RFC – sorry, we only had KSK 2010 so there was no signal of KSK 2017 so we dismissed it. Well we didn't dismiss it, we kept on looking.

Then in – so we looked at B, D, F and L root traffic that was from VeriSign, our root zone management partner, looked at traffic for A and J root server, and we came to what same conclusion this, the circle that is around that line, we have no idea why this doesn't go down. Now this is a problem. This is a problem because we needed to understand the signal better.

Keep in mind, we got 4.2 million individual IP addresses on average to the root server, some root servers less, some root servers more. So we did the – another analysis until the day I had to leave for the RIPE meeting, which was the October the 24th because 27,000 signals and only 1631 reported (new)

trust anchor. The analysis is complicated because DNS is a messy system. What we noticed there are resolvers – sorry there are four behind resolvers that were validating while the resolvers would happily send us the trust anchor that it learned from these forwards.

Now, that kind of make the situation looks worse, right, because if something is obscuring a whole set of IP addresses then the sample so under instead of accurate. Also, we noted resolvers behind forward make the situation – sorry – they make the situation look better, sorry. Another problem is that dynamic resolver IP addresses, and there are quite a few to my surprise, they walk around in the network, day by day they have different addresses. So do you observe of a week, those seven different addresses, there is only one single system.

So we then actually looked at the configuration itself, the trust anchor signaling how that worked. It turns out (bin) reports trust anchors even if it's not validating. So (bin) when you have KSK 2010 but you decide it's not to do DNS SEC, it will still report that it has this old trust anchor. And it is probably a safe bet that it will not upgrade to KSK 2017.

There is also some confusion about the configuration statements in (bin), we knew that. Before RFC 5011, which is the automated update scheme, you could configure in (bin) for instance trusted keys and in those trusted key statements you would say this is KSK 2010. Later on when there's RFC 5011, the automated update scheme, you know, these different configuration statements and (bin) trusted (unintelligible) managed keys.

Now when you're new to DNS SEC, this might not be obvious. We also noticed that a lot of resolvers are basically signaling this key (tech) even though they're not validating at all, we can see that because they don't have to deal with (unintelligible). And then we are know of a few operator errors where they basically restart the process everyday basically to empty the

cache. But because they do this every day, the RFC 5011 mechanism starts all over so you will never reach the 30 days.

So we were always worried about these bucks and operator errors. We didn't have any evidence until now. We are still doing the analysis. We hired a contractor, someone well known in the operator world, in order to figure out these reasons for misconfiguration he will contact various automated system numbers, he's starting with a sample of 500. Now this 500 – initially naively we said we should publish these addresses, maybe that helps people. But that was very naïve.

We immediately – if you do an IP to (ASM) translation basically you see the names of incorporations involved, you really don't want to name and shame them so that's not done. So we're not going to publish these addresses. And I think that's a healthy choice.

Analysis is ongoing as I said, this is a rough process indicator. Don't take too long to look at the slide – don't take too long to look at the slide, this is 40% is yet not contacted, 60% is contacted. Only 0.8% is resolved and this is from the initial 500.

Resolved (unintelligible) we have had for configuration, one is basically a resolve for forwarding to other resolvers. Another one is resolve for 5011 but could not write the journal file to this. These are common operator errors. And lastly, someone had the KSK 2010 configured manually without RFC but he was thinking this is actually RFC 5011 so it's a wrong trusted key statement. So back to the planning process, keep in mind that – sorry, first 19 September we did due diligence there, we looked at the traffic rates, we didn't see anything go up so we would continue.

Meanwhile we had received VeriSign's report, that one slide, and we covered it with our own data. And both VeriSign and ICANN we realized that we did not know what (unintelligible) was. Yes it was – it would tell us which trust

anchors were configured but we didn't know it was the original resolver if the resolver is validating, if there's backend signaling or if it's operator error.

I don't know if you've done things differently or we knew these were only operator errors but we know these are not only operator errors, these are also (unintelligible) implementations. So we looked at our operational plan, what our choices were. From day one we would follow operational plan, we wouldn't go do things ad hoc. So from the operational plan, we had the root zone management partners might also decide to extend any phase for additional quarter. For example if new information indicates that the next phase may lead to complications, the current phase would be prolonged. This is referred to as an extend scenario.

This report was – I'm sorry, the operational plan was published a few years. I'm not exactly sure what the date was, had community review. It was a big decision to do but we decided to have this extend scenario kick in. And we decided this on 27th September 2017 and we immediately went public with that information.

Again, we do not know how many validators are reporting key (tech) data compared to all validators, only very modern validation software will report this. Validators are not end users, or end systems, and of course the impact to end users is what is most important. So one of the things that we are going to do is compare our data with APNics Google ad experiment network. They have a ballpark estimate of numbers behind resolvers, sorry, of users behind resolvers which would give us an indication of how serious the situation is.

Mitigation is hard, we don't know – I'm sorry, we have already had a multiyear campaign to reach operators. Next steps, this is not about percentages, I want to make clear. We postponed the KSK roll until we get more information and understand the situation better. The delay is also at least one quarter. We can't do anything else, we can't do three weeks, we can't do five months.

This is because the key signing ceremonies that ICANN is holding every three months is kind of set in stone.

So we need to do this on a three month – on a quarterly or sorry – one or more quarters. We will at least partially mitigate, we hired the contractor to contact these 500 resolvers. And data collection continues, there's one message I want to bring to the table as well, we already have people unconfiguring so removing the KSK 2017 because the roll is not continuing. That's not the case. The roll will continue. Please do not remove, okay, remove KSK 2017. We have no date yet when we are going to roll.

Thank you. My apologies for this monotone session but I just came from the infirmary, they said go to bed, but we did this first then go to bed. Sorry.

Farzaneh Badii: Thank you very much. Rafik, please.

Rafik Dammak: Okay. Okay thanks for the presentation. I can acknowledge that it's always challenging to explain about DNS SEC even for technical people. So just quick question, we've got next steps, what will be the criteria for you to resume the process, I mean, the rollover here? Because I understand that you don't have a clear idea what the cause because when we talk about misconfiguration I mean, misconfiguration for anything networks, unfortunately common between many operators, that's not something you knew, not all of them follow the best practices. So what are your, I mean, kind of criteria because at some time I guess you need to decide how you move. We don't know – we don't need an IPv6 I think so.

The other just maybe technical point, I saw that you in term of misconfiguration you mentioned the (docker), I'm kind of surprised because (docker) container even if it's trendy now it doesn't look it's usually used for anything related to infrastructure. So how could you detect maybe that as a possibility? And just to make final comment, I want to thank you guys for the work. In term of communication I think it was done but even for me working

for a cloud provider, I find the information and the folks I work around, they were working to assess the impact of the KSK rollover and it was even funny that my boss calls me – I am the ICANN expert there.

But just in term that the information was there, but little comment about the material that you shared, it was little bit hard to find the information that you have the only those who are implementing DNS SEC I think it's maybe a resolver, name server that may be impacted, and so on. There was only one material that it's clear what are the cases that you need to be sure that – to get the update. So maybe if you want to rework your material to make it more clear for operators.

Roy Arends: I'll start from the first question, I think your first question, what are the criteria to move to an actual – is that correct? So honestly we want to understand the signal. If we can tie the signal down to only misconfigured resolvers, then I'm sorry, we have another two to three year outreach campaign. This has gotten some use as well but will be later on. There is not much we can do. I've talked to the ISPCP folks this afternoon, we have many different outreach campaigns about this.

At one point we will have to roll. If you're looking for a percentage, is 4% good enough, is 3% good enough? It's almost like this philosophical question, right, do you divert the train to drive over three workers or are you going to continue to drive over five workers? You know, it's – we delayed not because the percentage was high, we delayed because we didn't understand the signal.

So to answer your question, I don't know what the actual criteria are, we will roll at some point. We will announce (unintelligible) when we're going to roll. But to be honest, I don't know what the criteria are as of yet. Keep in mind this is only a few days after we decided to roll – to stop the roll.

Then the second it was about (docker), we didn't know it was (docker). The personal contact is one of these IP addresses. Got confirmation that they have this (docker) system in place and the consultant can only work with information that he gets from the operator. So this was new to us as well, but it's a category so we've added that, that's why you see it on the list.

The third point was a thank you, yes, you're welcome. And the fourth point we know there are definitely more cases because there are very strange signals. I can give you an example right now, we have a bunch of validators that not only reports the KSK 2017 and the KSK 2010, which is good, that's what you need, right? But they also reporting the ZSK for core 3. That's a bit weird because you don't configure a zone signing key as a trust anchor, because you roll these every three months, why would you do that?

The signal is so significant it is not high, but it's at least a signal (unintelligible) percentage that we think there's a tool out there that needs to be fixed. We don't actually need to fix that tool before rolling forward because it does KSK 2010 and KSK 2017, but yes, there were probably many more cases. We will find this out once we contact all of these addresses.

Now also keep in mind it's really hard to find humans associated with an IP address, so what we do is we translate that to an autonomous system number, we get the contact information from the autonomous system number and then we try to contact these people. Thank you.

Farzaneh Badii: Thank you very much. Seems like there's no other comment or questions.

Milton Mueller: Okay so you don't want me to ask that question, I won't. Just curious, is it – do people really use DNS SEC? I mean, is it actually being implemented in a widespread way such that I mean, it's somewhat disturbing how brittle the system was that, you know, sort of like the transition to digital television or IPv6 where you're afraid to turn off the old system because suddenly people

will be cut off? How much of a problem is this going to be going forward or does it matter because no one's using DNS SEC?

Roy Arends: From – to answer your first – well there's only one question, how many people are using DNS SEC I think, is DNS SEC widespread? We noted most of the top level domains are using DNS SEC, the root is signed. Those statistics you can all ignore, there's a one interesting statistic which is from (Jeff Houston)'s Google ad network, the has very clever way to measure who is validating and who is not, and hi number is 750 million browser impressions, sorry, unique IP addresses.

Now 750 million I don't know to how many resolvers that translate. But to me that's significant. I – that's basically my answer, so 750 million people are using it – are behind the resolver that's validating. That's different from that these people actually know that they are behind, I recognize that. And last thing we want to do is to – is to cut these people off from the Internet and that's why we delayed the KSK roll.

It's not surprising – you say it's surprising to you that the system is very brittle. It is not that brittle, but we can go back and forth and argue about this, so let's not.

Farzaneh Badii: Thank you very much. And we are done. Thank you very much for all – thank you very much, (Ray), for coming here.

((Crosstalk))

Farzaneh Badii: No, no she doesn't have a crush over me. Yes, no. Okay Joan, go ahead.

Joan Kerr: Great, thank you. We, as NPOC, would like to give Tapani a present because he's been – he's totally going to be surprised by this – for his support to us and – but we are also including a brochure so that – and you're not allowed to throw it out. So I'd like to give you that present.

((Crosstalk))

END