CONTENT OF CHAT – NBO Meeting -
DNSSEC WORKSHOP

Date:
Wednesday, 10 March 2010 - 09:00 - 12:00

Room:
Aberdere

Presentation:
.ORG DNSSEC
DNSSEC Deployment Update
DNSSEC Deployment in Europe
AfTLD DNSSEC Survey
Open DNSSEC
Overview of Open Source Tools for DNSSEC
Rollover and Die?
DNS/DNSSEC and Domain Transfers: Are They Compatible?
DNSSEC for the Root Zone

Meeting Leaders : **Julie Hedlund**
Director, SSAC Support

http://nbo.icann.org/node/8924

[08:49] Jim_Galvin: I hear the audio.
[08:56] Jim_Galvin: I hear the audio again.
[08:57] Jim_Galvin: Will they be connecting the teleconference?
[08:57] Jim_Galvin: Ah there it is.
[09:00] Doug_Barton: heh, wrong continent :)
[09:01] Doug_Barton: Can someone tell Julie that she doesn't have to speak directly into the mic? :)
[09:04] Jim_Galvin: Doug, what do you mean? I don't hear her unless she speaks into the mic.
[09:05] Doug_Barton: She had her mouth practically on the mic itself, produces a lot of distortion
[09:07] Samuel: that mic sounds good.
[09:08] Jim_Galvin: Yes, we are on the conference call and hear you.
[09:08] McTim: sounds good in acrobat!
[09:09] BrettCarr: Sound is good here
[09:09] Olof_Nordli: testing
[09:09] Samuel: Russ is very faint.
[09:13] Olof_Nordli: testing
[09:14] Jim_Galvin: The slide deck sent to dnssec-deployment was just the agenda slide, not the full deck.
[09:15] markus2: Jim, you can download the slides from the meeting website http://nbo.icann.org/node/8924

[09:15] Jim_Galvin: Yes, thanks, I know that. I just wanted Julie to know she had not really sent the slide deck to the mailing list.
[09:16] Jim_Galvin: Actually, all the slides are not on the web site. Seems mine aren't there for some reason.
[09:18] Jim_Galvin: Hmm, I was looking at a different node for this workshop that does not have all the slides. The one markus2 offered does have all the slides.
[09:20] Jim_Galvin: Thiery Moreau was the second to last name.
[09:44] BrettCarr: What Criteria would cause you to decide that things were broken enough that you would stop/rollback deployment?
[09:48] BrettCarr: Thanks Kim
[09:52] Jim_Galvin: Is SHA256 tested with the use of DURZ?
[09:53] Doug_Barton: Question: Is there somewhere that I can download a copy of the DURZ signed zone?
[09:53] Doug_Barton: (Sorry if I've missed it)
[09:53] BrettCarr: You can just axfr it can't you?
[09:53] Doug_Barton: Not yet, none of the servers that have it allow axfr
[09:54] BrettCarr: Some of the root servers are open for AXFR
[09:54] Doug_Barton: Thanks!
[09:58] BrettCarr: Doug: It's NSEC signed so you could also "walk" the zone
[10:01] Doug_Barton: Yes, I know that, but it doesn't give the whole zone (for example)
[10:01] Nick_Ashton: Seem to have an audio issue
[10:02] ICANN__Came: We're looking into it now Nick
[10:02] BrettCarr: Audio is fine here
[10:02] Nick_Ashton: thanks, wanted to make sure people knew there might be an issue
[10:02] Rick_Wilhel: If you lose audio, just leave and come back. (That worked for me)
[10:03] ICANN__Came: Everything appears to be fine from here as well. have you tried to reload Nick
[10:05] Doug_Barton: I actually hear some distortion on the audio, but it's not overwhelming
[10:06] Michele_Ney: same here
[10:06] Michele_Ney: but it's fine
[10:12] Jim_Galvin: Teleconference lost the room!!
[10:12] Michele_Ney: yeah
[10:12] Jim_Galvin: Ah, it's back.
[10:26] Michele_Ney: what if the client hasn't paid??
[10:27] Jim_Galvin: The assumption is that H is well behaved. If they are not then all bets are off I would say.
[10:27] Michele_Ney: Jim - H = holder?
[10:27] Jim_Galvin: Yes, registrant - domain holder.
[10:27] Michele_Ney: Jim - main problem with all of this is that it can only work in a very limited set of circumstances
[10:28] Michele_Ney: registrants don't update things until the last minute
[10:28] McTim: That sounds right Michele, fiendishly complicated
[10:29] Michele_Ney: McTim - I think I was meant to be the one in this session poking holes in the

entire thing :)
[10:29] Jim_Galvin: It is true that if H does not execute the steps they need to at the correct time, then things won't be smooth. This is no different than today, strictly speaking.
[10:29] Jim_Galvin: All DNSSEC does is shed a very bright shiny light on this process.
[10:29] Rick_Wilhel: Well put Jim ;-)
[10:29] Jim_Galvin: If you want to keep security then it is important to do it right.
[10:30] BrettCarr: But isn't the answer to make it clear to registrants (who want dnssec) that if you don't abide by these proceses you will see breakage
[10:30] Jim_Galvin: Yes, you are correct.
[10:30] Jim_Galvin: In fact, registrants already see breakage during registrar transfers.
[10:30] BrettCarr: The processes need to be clear and understandable (A largw Challenge)
[10:30] Michele_Ney: Brett - yes - basically tell them it won't work
[10:30] Jim_Galvin: It's commonplace.
[10:31] Jim_Galvin: One reason why Olafur is suggesting letting the new DNS operator to the process for you is an option.
[10:31] Jim_Galvin: But this requires the "technical conntact account" to work best, which is itself a new concept.
[10:31] Michele_Ney: his comments about transfer policy - that is in direct breach of IRTP
[10:32] Michele_Ney: ie. the current gTLD transfer policy
[10:32] Jim_Galvin: Say more?
[10:32] Michele_Ney: if a registrar did that they'd be in breach of current policy
[10:32] Jim_Galvin: Oh, you mean denying the transfer.
[10:32] RussMundy: as an individual, I have wanted to move some names from one registrat to another and found it it surpising difficult - right now it's on hold since I don't have time to deal with it
[10:32] Jim_Galvin: right?
[10:32] Michele_Ney: Jim - we can't NACK a transfer based on ANY of that
[10:32] Jim_Galvin: Right,
[10:32] Jim_Galvin: Olafur has his opinion. :-)
[10:33] Michele_Ney: Now if you want to change IRTP - work away, but it ain't going to happen anytime soon
[10:34] Jim_Galvin: For now, what I expect will really happen is that gaining registrars will make adjustments.
[10:34] Jim_Galvin: Those that add DNSSEC will add those adjustments.
[10:34] Michele_Ney: Jim - they can't adjust ICANN policy
[10:35] Jim_Galvin: You don't have to.
[10:35] Michele_Ney: is Roy in the room?
[10:35] Jim_Galvin: Olafur said that O registrar could refuse to transfer if you are signed.
[10:35] Jim_Galvin: I'm saying that's nice but I agree it won't happen any time soon.
[10:35] Jim_Galvin: It's also not necessary as long as H does what's right.
[10:36] Rick_Wilhel: Registrars face lots of scrutiny about behavior regarding transfers.
[10:37] Michele_Ney: Jim - the problem with all this is that you basically end up with a tiny subset of registrars and registrants being able to do anything

[10:37] Michele_Ney: Rick - so true. Compliance are about to audit us all for IRTP
[10:38] Jim_Galvin: It's only "tiny" until we get critical mass of registrars that offer DNSSEC.
[10:38] Rick_Wilhel: yes... perhaps based on NACK percentages... making this situation problematic... issue a NACK to keep the name working for H and it makes the registrar look as if it's misbehaving
[10:39] Michele_Ney: Rick - NACKs are one of the key things that they're looking at - and as already said DNS is not a valid reason to NACK
[10:39] Michele_Ney: Jim - you won' tget critical mass any time soon - there's no business case for most of us to implement it
[10:40] Rick_Wilhel: Michele: yup (I saw the Compliance preso yesterday)
[10:40] Jim_Galvin: What should happen is that H with the N registrar does not initiate a transfer until the DNS is ready at the N registrar. So there is no need for a NACK.
[10:40] Michele_Ney: Rick - which one? Registrar one or another one?
[10:40] Rick_Wilhel: Registrar
[10:41] Michele_Ney: Rick - so you'll have heard us whinging :)
[10:42] Rick_Wilhel: :-)
[10:44] Michele_Ney: Roy is one of the few DNS gurus who can actually explain stuff in a way that I can understand
[10:45] Jim_Galvin: Yes. This is great stuff!
[10:45] Doug_Barton: d'oh
[10:46] Rick_Wilhel: The quality of these slides is setting a VERY high bar! Graphics... animation... great content... clarity.
[10:46] Doug_Barton: video/audio is pausing
[10:46] McTim: yes, but i get lots of buzz on his mic
[10:47] JAco_vd_Wes: any questions you want to ask the presenter ?
[10:47] Michele_Ney: Jaco - not Roy. The previous guy - yes
[10:49] Suzanne_Woo: <ISC hat on> this is a ittle prejudicial, Roy....I don't find assertions like "irresponsible" terribly helpful.
[10:49] Michele_Ney: lol
[10:50] Suzanne_Woo: The patch in question is under test as we speak and will be widely announced when it's been tested enough that we won't be reproached for releasing untested bug fixes. :) (next couple of weeks.)
[10:51] BrettCarr: Does any other resolver code show similar problems, or is this a bind only problem?
[10:55] Jim_Galvin: If you check out this
[10:55] Suzanne_Woo: Brett: nsd also displays similar behavior although not quite as aggressively IIRC. (My apologies, it's 3am for me)
[10:55] Jim_Galvin: http://www.potaroo.net/ispcol/2010-02/rollover.html
[10:55] Jim_Galvin: They also mention UNBOUND.
[10:56] Suzanne_Woo: right, thx Jim
[10:56] Michele_Ney: lol
[10:57] Jim_Galvin: The problem exists elsewhere. I think Bind is the focus because it has such market share and is pretty aggressive as far as this issue is concerned.
[10:57] Michele_Ney: Roy isn't the most diplomatic - yet another reason why I love the guy

[10:57] Suzanne_Woo: I want to meet all the implementors who don't knowingly release software with bugs. I'd especially love to meet the ones who have released software.
[10:58] Doug_Barton: The bug was already present in all versions of BIND 9, releasing 9.7.0 and 9.6.2 had the advantage of giving users all improvements in those versions, without any detriment in regards to this bug
[10:59] Suzanne_Woo: Doug: thanks, that's exactly the rationale
[10:59] markus2: any questions for Olafur or Roy?
[11:00] Doug_Barton: I'm sensitive to Roy's point, especially as a registry op, but the releases don't make any existing problems worse
[11:00] Michele_Ney: For Olafur possibly
[11:00] Annabel_2: Suzanne: Don't worry about it. When all eyes are on you, you end up coming up with a better product.
[11:00] Michele_Ney: Tell Roy - he didn't
[11:00] BrettCarr: Very good and interesting presentation though :)
[11:00] Roland_van_: I have a question: Roy mentions all these issues as being caused by unintentional misconfiguration of resolvers. But what if this is exploited with malicious intent?
[11:01] Suzanne_Woo: Annabel: no worries here, it happens all the time. If we're not causing some kind of controversy, we're not doing enough. :)
[11:02] Suzanne_Woo: always a tradeoff....Roy's concerns are valid, so is the need to get other capabilities and bugfixes out while we fix this. As Doug noted, the basic issue has been present, not just in BIND, but for years. The critical path for the fix, it seemed to us, is "before the root is fully signed" more than "immediately and urgently,"
[11:06] Rick_Wilhel: For Olafur: On slide 14, you mentioned the distribution of TTLs (the variability of them, the median, etc)... is that data available?
[11:06] Roland_van_: What if you set up a botnet of malicious resolvers?
[11:06] Roland_van_: Thanks Roy
[11:07] Michele_Ney: Olafur - How do you expect to get buy in from registrars?
[11:08] Rick_Wilhel: Thanks Olafur... yes... doesn't need to be presented in real-time.
[11:08] Michele_Ney: Yes - I am the Blacknight :)
[11:11] Suzanne_Woo: I've got a few words on behalf of ISC when there's a moment
[11:11] Michele_Ney: with all due respect you're missing the question
[11:11] Michele_Ney: completely
[11:11] Michele_Ney: I asked basically "why"
[11:11] Michele_Ney: Why would a registrar want to implement this? It's not as if anyone is asking us for it?
[11:12] Michele_Ney: that's not much of an answer
[11:12] markus2: michele, is this OK?
[11:12] Michele_Ney: no matter
[11:12] Michele_Ney: markus2 - it's the same answer I always get :)
[11:13] markus2: ask him in personal next time in Brussel
[11:13] Kristian_Oe: Michele_Neylon: did you ask your customers? Our customers are positive about DNSSEC.

[11:13] Jim_Galvin: I missed the last few minutes on Adobe. My Firefox locked up.
[11:13] Michele_Ney: Kristian - you obviously have much geekier customers :)
[11:13] Jim_Galvin: I hear Russ on the phone.
[11:13] Peter_Larse: then you need to ask the correct question
[11:13] BrettCarr: i hear him but he is quiet
[11:14] Peter_Larse: the correct question is not: do you want more geeky stuff, but do you want higher security for your customers on their webshop
[11:14] Michele_Ney: Peter - no I don't. I'm not going to make more work for mysefl
[11:15] Michele_Ney: Peter - if you want to add complications and act as a beta tester - work away. I don't have the time or the patience
[11:15] Michele_Ney: Peter - most people don't even use SPF records .. can't see them using DNSSEC
[11:16] Jim_Galvin: I'll be saying shortly in the ORG presentation that there will be 10 registrars offering DNSSEC.
[11:16] Jim_Galvin: 10 is a far cry from the hundreds that exist but I can also say that not all of those 10 are small registrars.
[11:17] Michele_Ney: Jim - there are 2 types of registrars who might implement it
[11:17] Kristian_Oe: Jim_Galvin: i think the number of registrars will rise, when the ccTLD's starts to offer DNSSEC as well
[11:17] BrettCarr: I expect the demand to come from banks/finance/e-commerce some domains with less critical usage may never ask
[11:17] Michele_Ney: 1 - very big ones who have plenty of resources to play with stuff
[11:17] Michele_Ney: 2 - very small ones who like to play with geeky stuff
[11:17] Jim_Galvin: The ccTLDs who offer DNSSEC vastly outnumber the gTLDs that do already.
[11:18] Jim_Galvin: Michele: I agree.
[11:18] Michele_Ney: Brett - banks are targetted by phishing etc., yet most of them don't seem to even bother with SPF ..
[11:18] Peter_Larse: Michele: i do not consider myself to be in either one
[11:18] Michele_Ney: Jim - the problem is giving those of us in the middle a reason to do it
[11:18] Jim_Galvin: The problem with banks and email is as much about privacy as it is about authentication.
[11:19] Michele_Ney: Jim - yes, but if they used SPF it would be easier to block the spoofed emails before they hit anyone's inboxes
[11:19] Jim_Galvin: Michele: I think the market is going to sort that out. Either folks will want it and everyone will come on board (eventually) or there will always be a need for both.
[11:20] Jim_Galvin: I really want to believe that we all want better security, so we're all going to be on board eventually :-). It's really just a question of when.
[11:20] Peter_Larse: .. beeing a registrar with 200000 domains in dns, and actively testing and implementing dnssec for years, with limited resources
[11:20] Michele_Ney: Jim - maybe :) It's just the way some people see DNSSEC as being "the answer" to everything drives memad
[11:20] Doug_Barton: There are arguments about whether or not SPF is effective, but to the extent that it is, it's still a DNS record

[11:20] Peter_Larse: the whole SPF/domainskeys and SRS is an complete other discossion
[11:20] Doug_Barton: which means that it will benefit from DNSSEC
[11:20] Michele_Ney: Doug - key thing from our end is that it's easy to implement
[11:20] Michele_Ney: Peter - not really. SPF is easy to implement. DNSSEC transfers aren't
[11:21] Jim_Galvin: I agree that DNSSEC is not the answer to everything. It is, however,, a significant enhancement to a critical infrastructure protocol that will change the way the game is played.
[11:22] Doug_Barton: I don't think that it's the answer to everything, and I don't hear people saying that it is .... however it does actually solve a lot of problems that we have today, problems that need to be solved to handle more innovation
[11:23] Peter_Larse: Michele: no, SPF is easy to implement if you only look at the dns record, it's no longer easy when you realiaze that your mailservers have to implement SRS
[11:23] mib_1l6sb2: Michele, I think we can work out the process for transfer of signed zones to be clean, smooth and simple.
[11:37] Jaap_Akkerh: There is also a FreeBSD port
[11:39] tlr: note you need strong randomness when signing (for some signature algs)...
[11:40] BrettCarr: Yep so for critical zones use a (good) HSM
[11:42] Doug_Barton: Jaap, freebsd port of what?
[11:43] RussMundy: sorry, firefox locked up just as I saw an SPF & DNSSEC comment/question - We have tools to permit sendmail & postfix to do SPF DNSSEC validation
[11:43] Jaap_Akkerh: FreeBSD port of opendnssec
[11:44] Doug_Barton: ah, yes
[12:04] Kristian_Oe: .dk claims to be ready in July. I don't see them on the map
[12:05] Kristian_Oe: thanks
[12:05] mib_1l6sb2: Kristian, send me your email. Mine is steve@shinkuro.com
[12:06] Kristian_Oe: kristian@larsendata.dk
[12:06] mib_1l6sb2: :) Thanks. When I get a chance, I will send you the short set of questions and put the answers in my spreadsheet.
[12:06] mib_1l6sb2: For everyone, the questions are just the ones I mentioned
[12:06] Kristian_Oe: please notice. I'm not from the registry myself
[12:06] mib_1l6sb2: o Date when experimentation began
[12:07] mib_1l6sb2: o Date when there was a formal announcement that DNSSEC operation would happen sometme in the future
[12:07] mib_1l6sb2: o Date of partial operation, e.g. signing of the zone but not yet accepting registrations from the children.
[12:08] mib_1l6sb2: o Date of full operation.
[12:08] mib_1l6sb2: I will keep the answer confidential, if desired. Otherwise, I will include the info on my maps.
[12:09] mib_1l6sb2: Suggestions on how to improve the maps also welcome.
[12:13] Jim_Galvin: Thanks. Bye!
[12:13] Rick_Wilhel: Thanks Steve & Julie
[12:13] BrettCarr: thanks bye
[12:13] Jaap_Akkerh: Bye

[12:13] John_Demco: Thank you!