

DNS Vulnerabilities and Risk Management: A Discussion with the Experts

<http://brussels38.icann.org/node/12697>

Monday 21 June 2010 – 11:00 – 12:30

[2010-06-21 11::06:29] Bob_Connelly12671: Getting ready?

[2010-06-21 11::11:46] Bob_Connelly12671: That's good news

[2010-06-21 11::12:19] tlr: high-bandwidth audio stream has Bach?

[2010-06-21 11::13:00] Bob_Connelly12671: J S Bach? Tha't not what I hear.

[2010-06-21 11::14:40] tlr: Bob, what stream are you using?

[2010-06-21 11::19:32] Paul: Why is the DNS Vulnerabilities and Risk Management discussion delayed?

[2010-06-21 11::22:37] Robert_Hoggarth: Welcome to the session everyone!

[2010-06-21 11::23:19] Robert_Hoggarth: AS the in-room advocate for remote participation for this session I will be happy to read your questions live later in this session.

[2010-06-21 11::43:29] Robert_Hoggarth: As Rod's remark suggests, please start to send me any questions or comments you may have. thanks!

[2010-06-21 11::45:16] Robert_Hoggarth: A rare opportunity with a panel of this caliber

[2010-06-21 11::47:30] boggits: Do the panel think that the work in preparation by the community to deal with the side effects of DNSSEC (e.g. higher packet sizes) has been sufficient, if not what would they suggest?

[2010-06-21 11::47:56] wseltzer: "What can we do to distinguish between true threats and scaremongering? (as a public, and as a technical community)"

[2010-06-21 11::48:59] orange: where does one find the panelist names and profiles

[2010-06-21 11::49:04] Bob_Connelly12671: I think Steve Crocker is addressing the need for ICANN Accredited Registrars to have a Code of Conduce (CoC).

[2010-06-21 11::50:22] wseltzer: NOOO!

[2010-06-21 11::50:44] wseltzer: that was a response to "if we're in the business of providing identifiers, shouldn't we be making them safer"

[2010-06-21 11::52:51] Duncan_Hart: It's about continuous improvement over time

[2010-06-21 11::55:24] rm2: audio feed seems to have dropped

[2010-06-21 11::57:37] Robert_Hoggarth: tec team checked. its live and connected here

[2010-06-21 11::58:15] Robert_Hoggarth: i am prepped to answer the question from boggits

[2010-06-21 11::58:26] Doug_Brent: Rob, isn't that ask?

[2010-06-21 11::59:20] Robert_Hoggarth: :-)

[2010-06-21 11::59:59] Robert_Hoggarth: i am prepped to ask wendy's question, unless she intends to ask it in-person wendy?

[2010-06-21 12::00:17] hta: is there a way to connect to this channel using a normal irc client? I know I'm weird....

[2010-06-21 12::00:29] wseltzer: Robert_Hoggarth: I'm up at the mic, thanks

[2010-06-21 12::00:54] wseltzer: hta, yes chat.icann.org, this is #goldhall

[2010-06-21 12::02:05] hta1: thanks!

[2010-06-21 12::02:18] Robert_Hoggarth: hta, wendy beat me (and th tech team) to the answer! thanks wendy! :-)

[2010-06-21 12::03:41] KK: but what of the issues Paul is discussing are in the scope of ICANN?

[2010-06-21 12::03:50] Carmelo_Zaccone: Does the deployment of DNSSEC combined with DynamicUpdate might accelerate IPv6 deployment ? If so, what are the main 2 reasons of it?

[2010-06-21 12::05:49] hta1: ... that seem to offer a higher level of security ...?

[2010-06-21 12::05:51] Robert_Hoggarth: got you in the queue carmel - after KK

[2010-06-21 12::06:09] Carmelo_Zaccone: Thank you! Robert

[2010-06-21 12::06:16] Captain_ZOOM: Ironic, to increase Security an ISP will Disable/Block IDNs for their customers.

[2010-06-21 12::06:43] hta1: captain zoom, why?

[2010-06-21 12::06:50] Carmelo_Zaccone: Unfortunaltely I'm on the (left) corner room so no access to on room mike :(

[2010-06-21 12::07:25] Robert_Hoggarth: one of the benfits of Adobe Connect. helps remote AND in-person meeting attendees

[2010-06-21 12::08:05] Carmelo_Zaccone: On my side I do thing that DNSSec+Dyndate would stenght end host authentification and enforse then overall Internet security

[2010-06-21 12::08:23] Captain_ZOOM: DNSSEC is the world's most expensive Check-Sum

[2010-06-21 12::09:25] tlr: DNSSEC binds two identifiers to each other (IP address and domain name). It does not bind domain name to content. Therefore, user-facing DNSSEC indicators are a bad idea.

[2010-06-21 12::09:27] Captain_ZOOM: BGP is the largest Security issue of the public Internet - outside of the naive architecture

[2010-06-21 12::09:37] hta1: czoom: it's a keyed checksum, which is important. And it's cheap compared to pen-and-ink signatures :-)

[2010-06-21 12::10:23] Robert_Hoggarth: please remember to flag your posts at the beginning with QUESTION or COMMENT so I am clear on how to distinguish on-line chat from an interest in having me read something out loud

[2010-06-21 12::10:37] tlr: COMMENT: DNSSEC binds two identifiers to each other (IP address and domain name). It does not bind domain name to content. Therefore, user-facing DNSSEC indicators are a bad idea.

[2010-06-21 12::10:46] wseltzer: thanks Robert_Hoggarth (not a question :)

[2010-06-21 12::10:51] Robert_Hoggarth: if you start your post with one of those words - I will read it

[2010-06-21 12::11:00] Carmelo_Zaccone: we need to extend DNSsec not only to roots but also to edge DNS server to enforce host real identification thru their hostname (associated to their v6 IP address)

[2010-06-21 12::11:08] kris_r: how post a question? here?

[2010-06-21 12::11:29] Captain_ZOOM: DNS is NOT required to operate the Internet - DNSSEC is a joke

[2010-06-21 12::11:29] hta1: tlr, don't buy your argument. but that's a longer discussion, worthy of a beer.

[2010-06-21 12::11:57] Robert_Hoggarth: kris -- yes, unless you are in the room with easy access to the mic

[2010-06-21 12::12:44] Zahid_Jamil: QUESTION: What impact, if any, does DNSSEC have on filtering and blocking of domain names/web content?

[2010-06-21 12::13:00] Captain_ZOOM: Ask yourself, which is more secure Federal Express or the U.S. Postal Service?

[2010-06-21 12::14:20] Captain_ZOOM: DNSSEC was designed to break NAT edge devices with bloated packet sizes

[2010-06-21 12::20:29] Robert_Hoggarth: Reminder: If you start your post with the label QUESTION or COMMENT, I will read it out-loud here in the room

[2010-06-21 12::21:32] Captain_ZOOM: COMMENT would the people in that room be able to pass a basic Internet 101 test ?

[2010-06-21 12::22:55] Robert_Hoggarth: captain zoom. are you referring to attendees?

[2010-06-21 12::23:00] Duncan_Hart: If you can't Prevent something then you need to Detect, Respond and Repair

[2010-06-21 12::24:16] Captain_ZOOM: DH "Detect" that is very hard in the Naive Internet Architecture because Transit Time of Packets would have to be monitored and compared to an expected result - very expensive

[2010-06-21 12::24:42] Duncan_Hart: security is a cost and a performance penalty

[2010-06-21 12::25:17] Captain_ZOOM: a BGP Black-Hole ISP can capture traffic, record it, change it, and re-insert it and send it on its way and that takes TIME

[2010-06-21 12::25:19] Duncan_Hart: CZ - it depends on what is *really* important

[2010-06-21 12::25:46] wseltzer: agree with Crocker and would amplify: there's no way ICANN can (or should try) to produce a perfectly safe Internet

[2010-06-21 12::26:00] Duncan_Hart: CZ - it depends on what the business impact turns out to be

[2010-06-21 12::26:26] Captain_ZOOM: "perfectly safe Internet" is powered off

[2010-06-21 12::26:31] Duncan_Hart: perfectly safe is not achievable

[2010-06-21 12::28:59] Captain_ZOOM: The Internet is as safe and secure as passing written notes between desks in grade school with no teacher in the room

[2010-06-21 12::29:33] Robert_Hoggarth: glen ricart. noting your raised hand, you have to enter your question in this chat room labelled clearly with QUESTION or COMMENT if you would like me to read it out-loud in the room

[2010-06-21 12::30:18] Captain_ZOOM: QUESTION Do the people attending ICANN meetings have to pass any written test on Internet technology ?

[2010-06-21 12::30:46] Robert_Hoggarth: I can answer that - no

[2010-06-21 12::31:08] Duncan_Hart: QUESTION: Does the panel believe that it is possible to build systems with the three properties of: scale, functionality and 'security'?

[2010-06-21 12::31:35] Captain_ZOOM: QUESTION - Could a mentally retarded person who Wins the Lottery and has way too much time on their hands come and dominate ICANN meetings ?

[2010-06-21 12::32:12] Duncan_Hart: COMMENT: ;-)

[2010-06-21 12::33:56] Robert_Hoggarth: pending further consideration, i'll accept Captain Zoom's last question as a purely rhetorical one for future chat log reviewers

[2010-06-21 12::34:54] Carmelo_Zaccone: QUESTION: DNSSEC RFC is there for more than 5 Years now, WHY has it taken so long to start official initiative of deployment ??

[2010-06-21 12::35:08] Duncan_Hart: COMMENT: I am increasingly finding it hard to accept that the three properties are deliverable in one system. Case in point increased functionality does, IMHO, decrease levels of security

[2010-06-21 12::35:54] Duncan_Hart: COMMENT: Feature/functionality rich code has become increasingly difficult to gain trusted assurance in

[2010-06-21 12::36:03] Carmelo_Zaccone: End of 90' I was on first IETF meetings and I please but sad it took so long

[2010-06-21 12::37:57] Captain_ZOOM: DH: Thin-client vs. Thick-client debates will never end - Internet Architecture was supposed to be NO CENTRAL Servers and Single Points of Failure - DNS is Central Servers and Single Points of Failure

[2010-06-21 12::38:05] wseltzer: Robert_Hoggarth: Thanks for integrating the remote participants so effectively

[2010-06-21 12::38:31] guest: Nicely done remote participation - thanks!

[2010-06-21 12::38:41] Duncan_Hart: COMMENT: Whit also brought out the example of signing poorly developed code

[2010-06-21 12::38:44] Captain_ZOOM: "remote participants" what does it mean to be remote ?

[2010-06-21 12::39:00] Robert_Hoggarth: Sounds like we've run out if time. feel free to add any final comments in this chat for the next couple of minutes.

[2010-06-21 12::39:22] Duncan_Hart: COMMENT: and Whit's poorly developed code is exactly my point

[2010-06-21 12::39:32] Duncan_Hart: Rob_H thanks for your support

[2010-06-21 12::40:06] Captain_ZOOM: Who is "wendy" don't see a wendy on the list of 47 now 41