From: "Paul Hoffman" <paul.hoffman@gmail.com>
To: <DNSSEC@ntia.doc.gov>
Date: Wed, Nov 12, 2008 1:22 PM
Subject: Comments regarding the signing of the DNSSEC root

Date:
November 12, 2008

To:
Office of International Affairs
National Telecommunications and Information Administration

Greetings. We write this as a group of Internet technologists who work with DNS in general and DNSSEC in specific. We are concerned that the many questions in the Notice of Inquiry suggest that the NTIA may spend a long time deciding who should be signing the DNS root zone, carefully balancing the competing interests of the various stakeholders who hope to have the role of the signer of the root. Although we recognize that the "who signs" issue is not trivial, any delay at this point will have serious negative consequences for the DNS beyond simply postponing the security benefits of a signed root. Several top-level domain registries have already begun (or announced that they will soon begin) signing their domains individually, and more are likely to do so. The proliferation of individual TLD trust anchors makes the eventual transition to a signed root both more difficult and more dangerous.

We believe that having the root zone signed soon by an entity already trusted by the Internet users is much more important than spending years picking between the various parties who want the job. It doesn't matter to the Internet's users which of the two parties who are currently trusted -- IANA and the group of root server operators -- should sign the root zone. Very few users, even those running recursive name servers, know the difference between these two parties, and we think that is a sign that there is good stability in the operation of the root. What matters is that the root zone start being signed in a stable and secure fashion before the stability of the DNS is weakened by having too many TLD trust anchors in the configuration files of the recursive name servers throughout the world.

Already, some countries' TLDs, as well as .gov and .org, have announced that they intend to make trust anchors available so that they can secure their zones. While doing this makes sense to the zones themselves, we believe that the transition from a DNS where there are many trust anchors to a DNS with a single trust anchor (the root signed by a trusted party) will lead to unnecessary instability. Common DNS software has been shown to have surprising behavior when both a signed root zone and previously-signed TLD trust anchors are in the same configuration file; the more older signed TLDs there are before the root is signed, the harder the transition will be.

We note that, while it does not matter in a technical sense whether the signing entity is IANA or the group of root zone operators, it would matter to many people if the root zone was signed by an entity not currently trusted by the Internet users, such as an agency of some country's government, an agency of the United Nations, or a new multinational agency set up just to sign the root zone. There is already plenty of trust in IANA and in the group of root zone operators; having someone else sign the data that is already in the root would lead many Internet users (particularly ISPs running recursive name servers) to not trust the stability of the root itself, and that would be a very bad thing for the Internet.

In summary, please strongly consider simply allowing either IANA or the group of root zone operators to sign the root as soon as possible. The choice between these two is much less important than having this done sooner rather than later. Thank you for your consideration of this very important topic.

Sincerely,

Lyman Chapin
Paul Hoffman
Jelte Jansen
Frederico A C Neves
Jakob Schlyter
Andrew Sullivan
Paul Wouters