From: Brian Dickson <briand@ca.afilias.info>
To: <DNSSEC@ntia.doc.gov>
Date: Thu, Oct 9, 2008 2:39 PM
Subject: Re: Docket Number: 0810021307--81308--01

To:
Fiona Alexander,
Associate Administrator,
Office of International Affairs,
National Telecommunications and Information Administration,
U.S. Department of Commerce

To whom it may concern:

I have read the proposals in the appendices, and the FR summary article.

I am well versed in DNS operations, and DNSSEC in particular.

Disclosure: I am currently employed by Afilias, who operate a number of TLDs, including ccTLDs and gTLDs, including .org and .info.
However, my comments do not represent the position of Afilias, and are personal opinions only, albeit of a technical nature.

I have a number of comments on DNSSEC implementation on the root zone.

Note well - I do not believe any of the 6 current proposals adequately addresses concerns over the trust and security requirements which DNSSEC itself provides the means to facilitate. I have broken the flow of abstract components and entities down, identified the specific roles, and have listed some proposed rules on eligibility for any party to fulfill more than one of those roles.

I hope that this can help inform the evaluation process of bids for roles and for the overall design of the combined operation of the root zone.

Sincerely,

Brian Dickson
briand@ca.afilias.info

Comments in response to the questions posed

Q: In terms of addressing cache poisoning and similar attacks on the DNS, are there alternatives to DNSSEC that should be considered prior to or in conjunction with consideration of signing the root?

A: While there are other mitigation techniques available against attacks against the DNS infrastructure, as a general rule, they do not address the reliability and authenticity of the DNS itself. Those other techniques are orthogonal (unrelated) to the main benefits of DNSSEC, and as such, do not need to be tied to deployment of DNSSEC, either as an alternative, prerequisite, or co-requirement. The root should be signed, and that assessment is not dependent on other techniques.

Q: What are the advantages and/or disadvantages of DNSSEC relative to other possible security measures that may be available?

A: No other alternatives are currently ready for deployment or enjoy the widespread support of DNSSEC. No alternatives have reached the point in the long stands-development process within the IETF, which is widely considered a mandatory process before acceptance within the operator community on the Internet.

Q: What factors impede widespread deployment of DNSSEC?

A: The lack of a signed root zone, and to a lesser degree lack of speedy process for root zone changes, are the main impediments to widespread deployment of DNSSEC, and are very substantial impediments - this cannot be overstated.

Q: What additional steps are required to facilitate broader DNSSEC deployment and use? What end user education may be required to ensure that end users possess the ability to utilize and benefit from DNSSEC?

A: There would be value in, for example, a sponsored (or at least officially endorsed) interoperability test environment supported by the DOC. Some educational material for the lay person would be valuable, especially if hosted on an official government web site, such as NTIA, NIST, or similar authoritative entity.

Q: Should DNSSEC be implemented at the root zone level? Why or why not? What is a viable time frame for implementation at the root zone level?

A: Yes. Without a signed root, the trust issues surrounding trust anchors become significant, and key rollover becomes infeasible - itself a security concern. The viable time frame for the root zone should be 60 days or less, subject to MOUs on who operates which components, with open bidding processes for assignment of roles to follow. All of the processes for operation of components must be open. See below for further rules that I believe are important to ensure the integrity of the root zone and the security thereof are preseved.

Q: Is additional testing necessary to assure that deployment of DNSSEC at the root will not adversely impact the security and stability of the DNS? If so, what type of operational testing should be required, and under what conditions and parameters should such testing occur? What entities (e.g., root server operators, registrars, registries, TLD operators, ISPs, end users) should be involved in such testing?

A: No. The signing process is impacted by the rate of change of the root zone, which is currently on average less than a few times a day - well within the capabilities of even a modest consumer-grade computer. The use of DNSSEC, at all levels, is opt-in, so even in the face of potential stability issues resulting from root delegations with DNSSEC included, the opt-out solution ensures that the risk is well managed.

Q: How would implementation of DNSSEC at the root zone impact DNSSEC deployment throughout the DNS hierarchy?

A: It would accelerate and foster deployment of DNSSEC, and engender considerably greater trust in the DNS and its contents and operation.

Q: How would the different entities (e.g. root operators, registrarys, regisitries, registrants, ISPs, software vendors, end users) be affected by deployment of DNSSEC at the root level? Are these different entities prepared for DNSSEC at the root zone level and/or are each considering deployment in their respective zones?

A: All entities are either already prepared, with DNSSEC deployed, or will be unaffected by the signing of the root zone. Most entities are considering deployment, subject to the traditional curve of early-adopter, mainstream, laggards, in all spaces of the DNS ecosystem.

Q: What are the estimated costs that various entities may incur to implement DNSSEC? In particular, what are the estimated costs of those entities that would be involved in deployment of DNSSEC at the root zone level?

A: The costs involved are not negligible, but are manageable, as is demonstrated by the current deployment of DNSSEC in select TLDs. Again, opt-in ensures that only entities who need or want to, face incremental costs. The traditional cycle of obsolescence means that deployment of DNSSEC is not likely to present a substantial incremental cost over existing plans for upgrades at any entity.

Q: How should key management (public and private key sets) be distributed and why? What other factors related to key management (e.g. key roll over, security, key signing) need to be considered and how best should they be approached?

A: Key management, and management of the data itself, need to be very clearly delineated and separated. This falls into the area of traditional security, where the necessary elements to subvert the process are made as substantial a barrier as possible. This includes the potential for "hijacking" the process itself by holding the data hostage, by an otherwise trusted entity. Separation of management of root zone KSK and ZSK responsibility, equipment, and personnel, are mandatory in order to achieve that level of trust.

Q: Should multi-signature technique, i.e. M of N, be utilized at the root zone level? Why or why not?

A: Yes. Without M of N, there is risk to both the loss of access to keys, and risk of subversion of critical steps in the process. Suitable values for M and N have both technical and "political" sides to them, and should be selected based on a transparent process with input from both parties with direct interest, and parties who represent the interests of the consumers of the service, i.e. internet users.

List of functional roles, steps in the generalized root zone signing, and rules governing multiple roles

----

TLD Operator - send change request (including change to TLD zone DNSSEC key-signing-key)
IANA Functions Operator - processes request
Administrator - verify/authorize change request, and verify/authorize Key Update Request
Root Zone Maintainer - edit database/generate zone file
Root Zone Zone Signing Key Operator - generate ZSK, sign zone
Root Zone Distributor - distribute signed zone file to Root Server Operators
Root Server Operators - serve the signed root zone
Root Zone Key Signing Key Operators (multiple) - M of N required - generate KSK, publish public key, sign Root Keyset

Rules on separation of powers, data, trust:

(1) no one entity should have control over both ZSK and KSK
(2) no one entity should have control over unauthenticated changes (before Adminstrator) and authenticated changes (after Adminstrator, before signing)
(3) no one entity should have control over both the authenticated changes (after administrator) and signed data (after signing)
(4) no TLD operator should have control over any other TLD's changes, which basically is everything up to and including Root Zone Distributor
(5) no Root Server Operator should act as Root Zone Distributor exclusively - e.g. the RZD could be a shared function between multiple entities

Based on the rules above, none of the proposals meets the rules. Mostly this has to do with who manages the ZSK, and distribution of the signed zone.

I would be happy to explain any of these roles and rules in greater detail, if that would be of further assistance to the DOC or any party.

Sincerely,
Brian Dickson