From: Kentaro Mori <kentaro@jprs.co.jp>
To: <DNSSEC@ntia.doc.gov>
Date: Fri, Nov 21, 2008 11:44 PM
Subject: Comments concerning the DNSSEC signing of the root zone

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

To whom it may concern,

Greetings. I am Kentaro Mori of JPRS (TLD registry of .JP), currently in charge of the project for DNSSEC production implementation to .JP zone.

On behalf of JPRS, I would like to provide a feedback to your public comment request about DNS security of docket number: 0810021307-81308-01 in the Federal Register (October 9, 2008 Volume 73, Number 197, Page 59608-59612).

Please find the comments below, which are our thoughts basically related to your questions.

Comments with regards to Questions on DNSSEC Deployment Generally:

- DNSSEC is the technology that the Internet community has been cooperatively designing and verifying for a long time, carefully considering backward compatibility with the existing DNS, its performance issues, conformance issues with the current Internet structure and so on. We consider DNSSEC to be the only practical solution we are currently able to take to protect DNS fundamentally from data manipulation attempts.

- Therefore, considering the current situation, where the existence of apparent risks for DNS has been widely recognized, we support the immediate preparation of DNSSEC deployment. Without already knowing obvious ability to enforce DNS security, to start verifying other methods which replace DNSSEC or are combined with DNSSEC would be a waste of time and resources.

- To facilitate deployment, an effort by the root/TLD community to enlighten stakeholders (end users, software vendors, ISPs, Registrars, etc.) will be required, in addition to signing the root zone.

Comments with regards to General Questions Concerning Signing of the Root Zone:

- From the standpoint of properly moving the Internet forward with timely response to security demands, those who are involved in root DNS or TLD DNS administration have great responsibility to the community. Proactively deploying DNSSEC into the root/TLD zones would be one of the key elements in answering these demands and is considered to be the right thing to do in line with their roles.

- It would become difficult for users to replace their trust anchors with the root key if alternative technologies (such as DLV or ITAR) have been widely spread prior to the launch of the signed root zone. To deploy DNSSEC in accordance with the original design, signing of the root zone in the earlier deployment stage will be very important.

Comments with regards to Operational Questions Concerning Signing of the Root Zone:

- Operation flow should be designed so as to avoid the situation where a human error would lead to catastrophe, such as a whole TLD zone vanishing from DNSSEC-aware resolvers due to mismatching of TLD keys in a delegation point.

- Meanwhile, it is highly important that the operation flow has the ability to update the root zone immediately, especially in urgent situation such as the case of TLD key compromise occurring.

- The flow model that transfers root keys or zone data between multiple entities may have more difficulties than the other models, in keeping data security throughout the communication channels, operational efficiency for periodical root key rollover and rapid reaction capability in the event of emergent TLD key rollover.

- The purpose of DNSSEC deployment is to improve the current situation where DNS response can be malformed by unauthorized entities. Thus, it is desirable to implement a flow which extends naturally from the current one.

We hope this helps you move the deployment activities for the root zone signing forward to whatever extent. We also appreciate you giving us this opportunity.

Sincerely,

Kentaro Mori, Service Development department
Japan Registry Services Co.,Ltd. (JPRS)
E-Mail: kentaro@jprs.co.jp