From: "James M. Kretchmar" <kretch@akamai.com>
To: <dnssec@ntia.doc.gov>
Date: Mon, Nov 24, 2008 12:35 PM
Subject: Response to docket number 0810021307-81308-01

Date: November 24, 2008

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

Akamai Technologies is pleased to see forward progress being made on a supportable implementation of DNSSEC and we look forward to an end-to-end secure DNS.

We would like to provide the following technical comments in response to docket number 0810021307-81308-01, your notice of inquiry on "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System."

1. It is unclear how to manage DNSSEC when a third party is providing DNS hosting service for a registrant. In particular, the third party provider may need to request DS record updates with the registrar on behalf of the registrant. A standard mechanism should be in place to facilitate this interaction.

2. While we support the effort to deploy DNSSEC, we strongly encourage concurrent work on other strategies to enhance DNS security. For example, the "EDNS0 PING" proposal would go a long a way to protect against cache poisoning attacks. It is easy to implement and can be more rapidly deployed than DNSSEC.

3. The specification does not provide clear instructions for client behavior in the event that a non-root zone is rolled back from signed to unsigned. Clarification on this point will be important for implementing consistent client behavior.

4. We strongly support the deployment plan of an alternate root test bed, as described in the VeriSign proposal of September 22, 2008.

5. We recommend having multiple key signing keys defined and published as the root of trust, to increase the likelihood that client implementations can support multiple keys, as is necessary for key rotation (or "rolling the key").

6. We strongly recommend testing rotation of the key signing key on the root test bed before enabling DNSSEC on the production roots.

Andy Ellis - Senior Director, Information Security
James Kretchmar - Senior Architect, Mapping

David Lawrence - Senior Software Engineer, Mapping
Matt Levine - Director, Mapping
Jean Roy - Research Scientist, Mapping
Brian Sniffen - Senior Architect, Information Security