From: Vint Cerf <vint@google.com>
To: <DNSSEC@ntia.doc.gov>
Date: Mon, Nov 24, 2008 6:17 PM
Subject: DOC/NTIA DNSSEC Request for Comments

24 November 2008

Meredith Atwell Baker
Acting Assistant Secretary for Communication and Information Administration
National Telecommunications and Information Administration
Department of Commerce
Washington, DC

Via email: DNSSEC@NTIA.DOC.GOV

Reference: Docket Number 0810021307-81308-01
Enhancing the Security and Stability of the Internet's Domain Name and Addressing System

Dear Assistant Secretary Atwell:

With reference to your announcement in the Federal Register, Google is pleased to offer its response.

In simple terms, the root zone file today is assembled by the Internet Assigned Numbers Authority (IANA), which function is provided by the Internet Corporation for Assigned Names and Numbers (ICANN) under contract with the Department of Commerce. In the course of carrying out this task, IANA goes to substantial lengths to assure that any proposed or requested changes to the root zone file that it receives are thoroughly validated before they are sent to NTIA for review.

Once the review is completed satisfactorily, your authorized representative confirms this review to IANA and the changes are sent by IANA to VeriSign which uses the changes to produce a zone file for distribution to the Root Server Operators. VeriSign currently performs this root zone assembly and distribution function under contract to NTIA.

The need for and utility of introducing digital signatures into the root zone file have been amply outlined in your Federal Register notification and by many others. Google concurs with the view that it is timely and important to implement this process to increase the security of the Domain Name System.

After review of the several alternatives proposed in your notification, it is Google's view that the strongest and most expeditious way to introduce a digitally-signed root zone is to have the IANA generate the updated root zone file, sign it with an appropriate Zone Signing Key, produce the appropriate certificate validating this key with a Key Signing Key, and to send the assembled zone file to NTIA for review. Once this review is complete, the digitally-signed zone file would be sent to VeriSign for distribution to the Root Server Operators.

As should be clear, the digital signature does not encrypt any of the zone file contents but does allow any Domain Name System resolver to confirm the integrity of the response(s) to the domain name lookup. Thus the proposed root zone file contents can be reviewed by NTIA without difficulty. By keeping all digital signing operations collocated with IANA, the risk of alteration of the new root zone file is minimized and the party that is responsible for assuring the accuracy of the updated zone file, namely IANA, is also the party digitally signing the resulting zone file.

As nearly as I am able to tell, the process above appears to correspond to your Scenario 4. IANA has been producing digitally signed zone files for well over a year and, as its proposal shows, is prepared to undertake this task with the highest level of protection for the keys required for this process.

As many others have said, the need for this enhanced security is acute and I urge you and your staff at NTIA to proceed expeditiously to take the necessary actions to permit ICANN and VeriSign to move ahead rapidly to implement a digitally signed root zone file distribution system in accordance with the proposed procedures above.

Vinton G. Cerf
VP and Chief Internet Evangelist
Google

NOTE NEW BUSINESS ADDRESS AND PHONE
Vint Cerf
Google
1818 Library Street, Suite 400
Reston, VA 20190
202-370-5637
vint@google.com