

F-Root's DNSSEC Signing Plans

Keith Mitchell

Internet Systems Consortium
DNS-OARC

NANOG48, Austin, 24th Feb 2010

What is ISC ?

- Internet Systems Consortium, Inc.
 - Headquartered in Redwood City, California
 - 501(c)(3) Nonprofit Corporation
- Mission:
 - To develop and maintain production quality Open Source software, such as BIND, DHCP & AFTR
 - Enhance the stability of the global DNS through reliable F-root nameserver operations, and providing DNS-OARC secretariat
 - Further protocol development efforts, particularly in the areas of DNS evolution and facilitating the transition to IPv6.

Background

- DNSSEC has been around for many years
- Allows for cryptographic verification that DNS records are authentic
- Its time has finally come:
 - Standards and implementations are now mature
 - “Kaminsky” etc vulnerabilities
 - Many TLDs now signed or signing soon:
e.g. *.org*, *.gov*, *.se*, *.pt*, *.br*

Background

- DNSSEC is based upon a hierarchy of “trust anchors”
- The apex of these is the root
- Signing the root is necessary for full deployment
- Will allow DNSSEC-aware clients to follow a completely signed and verified delegation path
- ICANN finally agreed to have this happen in 2010

Background

- ICANN and VeriSign, with support from the U.S. Department of Commerce, have come up with the root signing plan and time-line, available at:
 - <http://www.root-dnssec.org/>
- The 12 operators of the 13 root server instances will be implementing this plan
- ISC is involved both as **F-root** operator and supplier of BIND software to several others

F-root Plans

- There are over 50 anycast instances of F-root globally, each with 2 servers:
 - <https://www.isc.org/community/f-root>



F-root Deployment Plan

- We will be upgrading all our F-root servers to BIND version 9.6.2 in support of a signed root during March
- 3-hour window between 21:00 and midnight UTC on 14th April to switch them all to DURZ
- Data gathering and submission to DNS-OARC during both our transition and all the other root DURZ transition slots

Side-Effects & Testing

- The (DURZ) “Deliberately Unvalidatable Root Zone”) provides opportunity for testing during the transition phase
- Network elements non-transparent to EDNS0 or large MTU UDP 53 may degrade DNS queries
- Testing tool provided by OARC at:
 - <https://www.dns-oarc.net/oarc/services/replysizetest>
- If you see issues, best to address them on your network ASAP, or there will likely be performance issues when signed root goes live on July 1st

Data Gathering

- During the transition, F and all but one other root operator will be gathering data to monitor for possible issues
- This will be uploaded and shared via:
DNS-OARC (<http://www.dns-oarc.net>)
- Various tools will be used to capture both long-term trends, and short-term snapshots during changes

What About DLV ?

- ISC's DNSSEC-Lookaside Validation service:
<https://www.isc.org/solutions/dlv>
was conceived as a transition tool to connect trust-anchor islands until the root downwards is signed
- We will continue to operate it as long as there are islands that need it, but will be very happy when the need goes away !

Summary

- Full plans/documents available at:
<http://www.root-dnssec.org/>
- ISC will be working with other root operators to transition F-root to the DURZ during the week of 12-Apr-10
 - More info at <http://blog.isc.org/>
- BIND 9.6.2 will be available by end February to support root operators
- Signed root planned to go live 01-Jul-10
- BIND 9.7.0 now available – try it if you haven't deployed DNSSEC yet !



BIND Versions

- ISC recommends and will be using internally a minimum consistent version:
 - BIND 9.6.2, released next week
- This has support for the SHA-2 DNSSEC algorithm used to sign the root
 - not strictly needed as root servers only serve signed zone as content, not validate it
 - but we want to be able to support a specific version for this
- Other root operators who use BIND are being encouraged to Beta test this version early

BIND Versions

- Latest version of BIND is 9.7.0, just released: *“DNSSEC for Humans”*
- It has many features to make deployment of DNSSEC within your network much more user-friendly
- Strongly recommend this version for your authoritative servers
- Recommend waiting for patch (*available in ~2-4 weeks*) for validating resolvers