



# DNSSEC This Month

ISSN 1932-6564

JUNE 1, 2007

VOLUME 2, NUMBER 6

Welcome to the June 2007 edition of *DNSSEC THIS MONTH*, a monthly newsletter about advances in securing the Internet's naming infrastructure in the government, business and education sectors. The [DNS Security Extensions \(DNSSEC\) Deployment Coordination Initiative](#), which produces this newsletter, is part of a global effort to deploy new security measures that will help the DNS perform as people expect it to -- in a trustworthy manner. This newsletter will offer updates on new policies, early adopters and advances in DNS security extension development. For more information on progress toward DNSSEC deployment, read the initiative roadmap at <http://www.dnssec-deployment.org/technology/roadmap.htm>.

The U.S. Department of Homeland Security Science and Technology Directorate provides support for coordination of the Initiative.

To subscribe, please send a message to [news-subscribe@dnssec-deployment.org](mailto:news-subscribe@dnssec-deployment.org)

To unsubscribe, please send a message to [news-unsubscribe@dnssec-deployment.org](mailto:news-unsubscribe@dnssec-deployment.org).

For more information, go to <http://www.dnssec-deployment.org/news/dnssecthismonth>

**New version of DNSSEC-Tools software suite now available:** Initiative partner SPARTA, Inc. has released version 1.2 of the DNSSEC-Tools software. The new version provides patches for enabling local DNSSEC validation in a number of applications, including Firefox, Postfix, Sendmail, Libspf2, Wget, Jabber-2, Ssh, and Ncftp. The validator library contains an expanded set of validator policy definitions, and provides initial support for Dynamic Lookaside Validation (DLV). Also included: the trustman utility, an IETF "Timers" compliant implementation for automated monitoring and updating of DNSSEC keys used as trust anchors at end resolvers. The tools available for zone signing and key (KSK and ZSK) rollover operations have also been noticeably improved. Find out more at <http://www.dnssec-tools.org>.

**New DNSSEC Pilot Program for US Government:** DNSSEC Deployment Initiative partners at the National Institute for Standards and Technology (NIST) and SPARTA Inc. are working together under guidance from the Dept. of Homeland Security to form a **new DNSSEC deployment pilot program for US government DNS administrators**. DNSSEC implementation and usage are among several new security controls that are part of the Federal Information Security Management Act (FISMA), which will form the basis of all federal IT security policies. The Security Naming Infrastructure Pilot (SNIP) was formed to help civilian US government agencies to deploy DNSSEC and test new operational procedures, with the goal of providing a distributed training ground where US government DNS administrators can deploy and maintain a signed test delegation before signing their actual production zones. The SNIP is composed of a central domain (dnsops.gov) with individual agencies delegated under it (for example, NIST would become nist.dnsops.gov). The entire dnsops.gov tree will be signed, and the SNIP key would become the trust anchor for the dnsops.gov domain.

As agencies gain more experience with new DNSSEC specific operations, they will migrate away from the pilot zone to deployment of a DNSSEC signed zone. The operation of dnsops.gov itself will cease when the General Services Administration (GSA) has the ability to maintain a signed .gov zone. In addition to being a pilot deployment within the civilian federal government, the **SNIP also will be a testbed for DNSSEC enabled software such as authoritative servers, validators, and DNSSEC-aware applications**. The goal is to mirror the current .gov domain as much as possible with regards to the various software products used within government IT. The SNIP pilot is open to all US Government agencies that need to meet FISMA controls and membership is strictly voluntary. Agency DNS administrators can request a delegation from the SNIP zone and are responsible for deploying and maintaining it; pilot zones should mirror agencies' actual DNS as much as possible, and may be used to develop and test operational procedures that meet FISMA controls for DNS security. Other resources, material and training classes will be part of the project as it progresses. For more information on SNIP and current project status, go to <http://www.dnsops.gov/>.

**CACM June issue includes DNSSEC:** The June 2007 edition of *Communications of the ACM*, the Association for Computing Machinery, includes the article "A Piece of the Internet Infrastructure Puzzle," describing the role DNSSEC can play in securing the Internet, by authors Amy Friedlander, Allison Mankin, Douglas Maughan, and Steve Crocker. Find the issue at <http://acm.org/cacm/>.

As of May 20, the SecSpider monitoring site shows 870 DNSSEC enabled zones

Editor: Denise Graveline  
Contact:  
[news-editor@dnssec-deployment.org](mailto:news-editor@dnssec-deployment.org)

**Tutorial: Inside tracking DNSSEC-enabled zones:** Measurement efforts such as the SecSpider project (<http://secspider.cs.ucla.edu>) show DNSSEC is growing (see numbers on the DNSSEC deployment website at <http://www.dnssec-deployment.org/zones/secspider.htm>). *DNSSEC This Month* asked Eric Osterweil, main developer of the SecSpider project, about what monitoring projects are yielding:

**Q: What does the current count on SecSpider tell us?**

**A:** Any current count is only an estimate. There are tens of millions of zones and a zone can choose to enable (or disable) DNSSEC at any time. It may take DNSSEC monitors some time to find the newly secure zone, if it is found at all.

**Q: Aside from tracking DNSSEC's progress, are there other benefits?**

**A:** Looking at monitoring practices leads to concrete steps that can be taken by both DNSSEC enabled zones and future monitoring projects.

**Q: How do monitoring projects find DNSSEC-enabled zones?**

**A:** The first and most effective way is for the zone to register itself with one of the monitoring sites. The SecSpider website has a form where one can submit the name of a DNSSEC enabled zone. If zones don't register themselves, monitoring projects attempt to find them using various methods for crawling the DNS. Given the vast number of DNS zones, it can take a long time before a DNSSEC enabled zone is discovered by a monitor. Zones that enable DNSSEC and coordinate with a DNSSEC enabled parent can be found more quickly.

**Workshops help networks, organizations, deploy DNSSEC:** While the protocols needed to add additional security to DNS queries and responses exist, network administrators and organizational leaders in all sectors need to accept DNSSEC and put it to use. Here's a roundup of speakers and sessions that may help you work through potential issues and concerns about deployment:

**Conference Call Symposium: DNSSEC Implementation Made Easy :** On June 6, at 3:00 pm EDT (1900 UTC), the DNSSEC Deployment Working Group will hold a conference call symposium on the hardware and software available for DNSSEC-compliant name servers. Speakers will focus on the registry perspective for all zones, based on experience deploying DNSSEC or providing deployment solutions at SPARTA, VeriSign, Secure64 Software, Xelerance, and Nominet. Presentation materials are available at <http://dnssec-deployment.org/wg/materials/20070606>. To join the call, the dial in numbers are: USA Toll Free Number: +1 888-221-7341, USA Toll Number: +1 973-935-2305, and the Passcode is: 599786#.

**Reminder! NANOG meets in Bellevue, Washington: June 3-6** are the dates for the NANOG 40 meeting, to be held in Bellevue, Wash. You can register here: <https://www.nanog.org/registration/>.

**Reminder! ICANN to San Juan in June:** The ICANN Annual Meeting for 2007 will convene in San Juan, Puerto Rico, **June 25 to 29**. ICANN meetings are free and open to the public. More information can be found at <http://www.icann.org/meetings/sanjuan/>.

**Reminder! IETF in Chicago:** The 69<sup>th</sup> IETF meeting takes place in **Chicago, Ill., July 22-27**. Online registration began March 21; a schedule of important meeting and pre-meeting dates can be found at <http://www.ietf.org/meetings/69-IETF.html>

© 2007. Shinkuro, Inc. All rights reserved.