



DNSSEC This Month

ISSN 1932-6564

JANUARY 5, 2007

VOLUME 2, NUMBER 1

Welcome to the January 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. Some 10 percent of servers in the network today are vulnerable to domain name system (DNS) attacks, and many experts expect a serious attack on the underlying infrastructure within the next decade. 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.

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

To unsubscribe, please send a message to news-unsubscribe@dnssec-deployment.org.

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

New report on Swedish tests of DNSSEC implementation: Sweden's National Post and Telecom Agency, Post-och Telestyrelsen, has issued a report on its tests of DNSSEC implementation and administration on a sub-domain to the .se-domain. The tests were designed to determine ease or difficulty of launching and running DNSSEC, support from the ccTLD, implementation steps to take and their order, and more, according to report author Anders Rafting. The Swedish top-level domain .se is the first national top-level domain in the world to introduce DNSSEC. The report notes that the **test results show that DNSSEC implementation "generally is easy to perform,"** adding that "What is missing today are good tools for automation of DNSSEC administration (key generation and zone signing). A standardization of such tools feels like a necessity for the usage of DNSSEC to take off." However, it calls DNSSEC "the right choice to achieve increased trust to the DNS and the Internet as a whole." Titled *Improved security of the Domain Name System* (Report number PTS-ER-2006:36), **an English-language translation of the report is available at no charge as a PDF at** http://www.pts.se/Archive/Documents/EN/Improved_security_DNS_Implementation_DNSSEC_2006_36.pdf.

FISMA Update: The U.S. National Institute of Standards and Technology (NIST) has announced the release of Special Publication 800-53, *Revision 1, Recommended Security Controls for Federal Information Systems*. This publication provides the first major update for the security controls selection and specification guidance since February 2005. Important changes to the Media Protection, Certification, Accreditation, and Security Assessments, and Identification and Authentication families are included in the update as well as new guidance on updating security controls and the use of external information systems. The guidance includes a plan for staged deployment of DNSSEC technology within federal IT systems, and specifies the mandatory minimum security controls necessary to comply with Federal Information Processing Standards (FIPS) required by the FISMA legislation. US federal agencies will have one year after final publication to comply with the new standards. For the full report, see: <http://csrc.nist.gov/publications/nistpubs/index.html#sp800-53-Rev1>

Economics of information security and DNSSEC featured in Science:

"Network insecurity is somewhat like air pollution or traffic congestion, in that people who connect insecure machines to the Internet do not bear the full consequences of their actions," write University of Cambridge researchers Ross Anderson and Tyler Moore in their paper *The Economics of Information Security*, published recently in the journal *Science*. Noting that "incentives are becoming as important as technical design in achieving dependability," the authors cite DNSSEC as an area of information security affected by externalities, situations in which individuals' actions have side effects on others. "A number of core protocols, such as DNS and routing, are considered insecure. More secure protocols exist (e.g., DNSSEC, S-BGP); the challenge is to get them adopted," the authors write. A free abstract of the article is available at <http://www.sciencemag.org/cgi/content/abstract/314/5799/610>, and non-subscribers to the journal also can order a copy of the article at that site.

NIST online resources offer tools for deploying DNSSEC: The U.S. National Institute of Standards and Technology (NIST) has several ongoing projects related to DNSSEC detailed on the project homepage: <http://www-x.antd.nist.gov/dnssec>. The project's main focus is the deployment of DNSSEC in the U.S. government IT sphere, but has **tools and information of interest to the broader community.**

“Today, more than 92 percent of critical business records are generated, managed and stored electronically, creating efficiencies and cost-savings for businesses. Unfortunately, digital information can be easily deleted, altered and/or manipulated. For businesses, the burden of proof is on the company to ensure and attest to the accuracy and credibility of their electronic business records.”

*-- Cyber Security Industry Alliance,
[Data Manipulation: Get the Facts](#)
November 2006*

Editor: Denise Graveline

Contact:

news-editor@dnssec-deployment.org

Included on the project webpage is a link to the NIST Special Publication 800-81 “Secure Domain Name System (DNS) Deployment Guide” along with online tools to test conformance to the guidelines in the Special Publication. Other online tools allow participation with the DNSSEC deployment community by volunteering the status of a zone (signed or unsigned) to be monitored. Also available: Results of the impact DNSSEC deployment has on server performance, along with a link to the tools used to conduct the tests, at <http://www-x.antd.nist.gov/dnssec/dnssec-perform.html>.

SPARTA Inc. releases version 1.0 of its DNSSEC-Tools software suite: The latest version of the software provides updated patches for DNSSEC-aware applications such as Firefox and Sendmail; an improved zone-signing utility that hides much of the complexity of key generation, key maintenance and zone-signing behind a simple command-line interface; a key-rollover utility for managing the graceful rollover of keys within a zone; a tool that provides initial support of the IETF “Timers” draft for automated monitoring of DNSSEC keys used as trust anchors at end resolvers; a new Perl interface to the validator library and numerous improvements to other helper modules and libraries. Also included are various operator guidance documents: for zone administration using the DNSSEC-Tools software, for DNSSEC troubleshooting, and for DNSSEC-aware application development. Download the DNSSEC-Tools software from <http://www.dnssec-tools.org>

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:

IETF meets in Prague: Prague, in the Czech Republic, will host the **68th IETF meeting March 18-23, 2007**. Details can be found at <http://www3.ietf.org/meetings/68-IETF.html>; important dates for submittal of agendas in advance of the meeting are at http://www.ietf.org/meetings/68-cutoff_dates.html.

APNIC 23 to Indonesia: The 23rd APNIC Open Policy Meeting (APNIC 23) will be held in conjunction with [APRICOT 2007](#) in Bali, Indonesia from February 26 to March 2. A draft program is available at <http://www.apnic.net/meetings/23/program/index.html>, and video streaming, audio streaming, live transcripts, Jabber Chat and podcast services will be available from February 28.

Joint Techs Workshop in Minneapolis: The winter 2007 [ESCC/Internet2 Joint Techs Workshop](#) will be held in Minneapolis, Minnesota starting Sunday, February 11 and ending Thursday, February 15. The three focal areas are Hybrid Networking, Campus Networks and Security. A very preliminary agenda – which may expand to include related meetings before or after the workshop – is at <http://jointtechs.es.net/minnesota2007/JT%20Minneapolis%20Prelim%20061030/JT%20Minneapolis%20Prelim%20061030.htm>.

© 2007. Shinkuro, Inc. All rights reserved.

DNSSEC This Month, Vol. 2, No. 1, January 2007, page 2

ISSN 1932-6564