



DNSSEC This Month

ISSN 1932-6564

OCTOBER 1, 2006

VOLUME 1, NUMBER 6

Welcome to the sixth 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 unsubscribe@dnssec-deployment.org.

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

Symantec tells U.S. Congress cybercrimes cost businesses \$48 billion in 2005: Symantec security response senior director Vincent Weafer testified in September before the House of Representatives subcommittee on telecommunications and the Internet that **attacks on the Internet infrastructure cost businesses \$48 billion and consumers \$680 million last year.** He also pointed to fewer, but more sophisticated, attacks that focus on weak spots in Web servers and applications, and called on Congress to invest in consumer awareness programs, more funding for cybersecurity research and development and law enforcement efforts including a national law against data breaches. Speaking of the need for more cybersecurity R&D, Weafer noted "we must do it together in partnership; industry government and academia alike. The Federal Government must **focus on funding cybersecurity R&D to meet the constantly evolving threats that face our nation's critical infrastructure.** And the Government must also lead by example, securing its own systems through the use of reasonable security practices." You can read more about Weafer's testimony in the *Information Week* article at <http://www.informationweek.com/software/showArticle.jhtml?articleID=193000551>, a copy of the testimony at <http://energycommerce.house.gov/108/Hearings/09132006hearing2022/Weafer.pdf>, and Symantec's most recent Internet Security Threat Report, cited in the testimony, at <http://www.symantec.com/enterprise/threatreport/index.jsp>.

Most damaging network attacks are preventable, according to a U.S. Department of Justice report analyzing prosecuted cases of cybercrimes related to network intrusion and data theft between 1999 and 2006. (Only publicly disclosed cases were analyzed.) The report shed light on the types of attacks discovered; the location and equipment used; the relationship, if any, of the attacker to the attacked organization; and more. The average financial loss per case: \$3 million. To read the report, go to http://www.net-security.org/dl/articles/Report-DOJ_Computer_Crime_Prosecutions.pdf.

CITEL newsletter covers DNSSEC: The latest issue of *info@citel*, the newsletter of the Inter-American Telecommunications Commission of the Organization of American States, includes an article on "DNSSEC: Protection You Need But Cannot See," from the DNSSEC deployment initiative at http://www.citel.oas.org/newsletter/2006/agosto/dns_i.asp. (A Spanish-language version can be found at http://www.citel.oas.org/newsletter/2006/agosto/dns_e.asp.) Based in Washington, DC, CITEL works under the auspices of OAS with governments and the private sector to advance development of the Americas via telecommunications. It includes 35 member states and more than 200 associate members.

Two RFCs now available. **RFC 4641 DNSSEC Operational Practices** sets forth "a set of practices for operating the DNS with security extensions (DNSSEC)" for zone operators based on workshops and early operational deployment tests. Written by experienced DNSSEC implementers **Olaf Kolkman** and **Miek Gieben**, both of **NLnet Labs**, the document examines operational issues concerning key generation, key storage, signature generation, key rollover, and related policies. Read the document at <http://www.rfc-editor.org/rfc/rfc4641.txt>. Also released is **RFC 4635 HMAC SHA TSIG Algorithm Identifiers**, by **Donald Eastlake of Motorola**. It addresses technical issues associated with authenticating one of the DNS records. Read the document at <http://www.ietf.org/rfc/rfc4635.txt>.

Over the last six months of 2005, Symantec detected an average of 1,402 Denial of Service (DoS) attacks per day. This is an increase of 51 percent from the first half of 2005, when Symantec detected an average of 927 DoS attacks per day.

--Symantec Internet Security Threat Report, Volume IX, March 2006

Editor: Denise Graveline

Contact:

news-editor@dnssec-

deployment.org



SecSpider the DNSSEC Monitoring Project



Monitoring tool shows early DNSSEC deployment in real time: The **SecSpider DNSSEC monitoring tool** at <http://secspider.cs.ucla.edu> provides a window into the early DNSSEC deployment and operations. SecSpider crawls the DNS name space looking for zones that have deployed DNSSEC and monitors their operations. The site, which also allows you to request monitoring of an as-yet undiscovered zone, has been **in use since mid-2005 and currently monitors over 118 secure zones**. For each monitored zone, SecSpider uses periodic DNS queries to monitor operational issues such as the type and number of DNSKEY records used by the zone, the signature lifetimes, the distribution of cryptographic algorithms in use, and key and record set rollover behavior. The interface offers displays of data from any DNSSEC zone, allowing operators of secure zones to see how others view it, practices in use by early adaptors, and a global view of DNSSEC deployment. For example, **SecSpider can be used to reveal the risks involved with different signing strategies, track the delegation consistency between parent and child zones, and describe islands of security**. A complete data set is available from <http://secspider.cs.ucla.edu/>. Secure-zone operators are encouraged to submit zones for monitoring and comparison with other operators' zones. If your secure zone has not been identified by the crawler, you may add it to the list on the website. Zones that may deploy DNSSEC in the future are also encouraged to register. For more information, contact Eric Osterweil (eoster@cs.ucla.edu) or Dan Massey (massey@cs.colostate.edu).

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:

- **Economic aspects of Internet security explored:** A workshop on the economics of securing the information infrastructure, sponsored by I3P, will take place **October 23-24 in Washington, DC**. **Steve Crocker** of Shinkuro will join a panel on economic barriers and incentives for DNSSEC deployment, and additional panels will explore the economics of corporate investments in cybersecurity, modeling the vulnerability black market and predictive modeling for security operations economics. Registration is free, at <http://wesii.econinfosec.org/workshop/program.php>.
- **Reminder! RIPE 53 to include DNS session:** The RIPE 53 meeting in **Amsterdam, October 2-6**, will include **sessions on DNS**. Registration and more information can be found at <http://ripe.net/ripe/meetings/ripe-53/>.
- **Reminder! The Air Transport Association of America** will feature initiative partners **Steve Crocker** and **Cathy Handley** in a session on "**Securing the Internet with DNSSEC**" at its next e-business forum **October 20 and 21 in Louisville, Ky**. The DNSSEC panel also will include speakers **Gary Cooper** of ARINC, an aerospace communications and engineering company and **Marie Zitkova** of SITA, which sponsors, operates and maintains the dot-aero naming structure. For more information visit <http://www.ataebiz.org/forum>.
- **Reminder! Next IETF in San Diego:** The **Internet Engineering Task Force** will convene its 67th meeting **November 5-10** in San Diego, California. Go here <http://www3.ietf.org/meetings/67-IETF.html> for more information.

© 2006. Shinkuro, Inc. All rights reserved.