DNSSEC In The Field

Improving the security of the Internet’s naming infrastructure

ICANN 34 | Mexico City, Mexico
Wednesday, 4 March 2009
0900 – 1230
Don Diego 3

Meeting Agenda

Welcome and Introductions

Steve Crocker, Russ Mundy
Co-Chairs DNSSEC Deployment Initiative

The DNSSEC Industry Coalition

Lance Wolak, PIR, Director Product & Marketing
Crystal Peterson, PIR, Marketing Communications

THE DNSSEC INDUSTRY COALITION is a global group of registries and industry experts whose mission is to work collaboratively to facilitate adoption of DNSSEC and streamline the implementations across Domain Name Registries. Members work together to establish a consistent set of tools and applications, shared best practices, specifications and shared nomenclature. DNSSEC Industry Coalition members include both gTLD and ccTLD registries along with industry and educational experts of the Domain Name System.

DNSSEC In The Field

.ORG DNSSEC Implementation Update
Lance Wolak

A brief status on .ORG's DNSSEC implementation with a focus on operational readiness and market conditioning activities.

IANA Interim Trust Anchor Repository Update
Kim Davies, ICANN, Manager, Root Zone Services

IANA is deploying an Interim Trust Anchor Repository for TLD keys.

Break: 1030-1100

Welcome and Introductions

Steve Crocker, Russ Mundy
Co-Chairs DNSSEC Deployment Initiative

European Commission High Level Internet Governance (HLIG) Summary of 5 February Brussels Meeting

Michael Niebel, Head of “Internet, Network and Information Security”, European Commission

The EC HLIG group met in Brussels on 5 February to consider the issues related to deployment of DNSSEC. The result was a spirited discussion of pros and cons.

DNSSEC In The Field

Comcast Validating Resolver Experience
Steve Crocker

Broadband Router Compatibility
Steve Crocker

Simplifying DNSSEC: The Need For a 1-Click Solution
Michael Young, Afilias, Vice President Product Development

DNSSEC Status Update

Steve Crocker, Chair SSAC

DNS Security

DNS security (DNSSEC) works by introducing digital signatures throughout the DNS infrastructure. It establishes that the binding between a domain name and its resource records, including its IP addresses, has not been compromised. It can provide users with effective verification that their applications, such as web or email, are using the correct addresses for servers they want to reach. It can also be used to provide authoritative evidence that a binding is bogus or that a specific domain name does not exist.

Zone operators use pairs of public-private keys to sign their zones digitally. Either individual zone administrators or DNS service providers then must host signed zones with a DNSSEC-compliant name server. Once compliant, applications such as web browsers and email systems can use the digital signatures to provide secure services to their users.

DNSSEC-based authentication is the key to identifying attacks and providing a distributed, secure naming mechanism that can be leveraged for new services. The DNSSEC Deployment Initiative works to encourage all sectors to voluntarily adopt security measures that will improve security of the Internet's naming infrastructure. This initiative is part of a global, cooperative effort that involves many nations and organizations in the public and private sectors. The U.S. Department of Homeland Security provides support for coordination of the initiative.

DNSSEC Resources

Information

The DNSSEC Deployment Initiative:
http://dnssec-deployment.org

DNSSEC Information Clearinghouse:
http://www.dnssec.net

DNSSEC Server Software

ISC's Bind 9
http://www.isc.org/bind

NLNetLabs NSD
http://www.nlnetlabs.nl/nsd

Nominum's ANS and CNS
http://www.nominum.com/products.php

Secure64 SW Corp DNS Server
http://www.secure64.com

DNSSEC Tools and Applications

SPARTA's DNSSEC-Tools and Applications
http://www.dnssec-tools.org

NIST Tools
https://www-x.antd.nist.gov/dnssec/download

RIPE NCC DNSSEC Key Management Tools
https://www.ripe.net/projects/disi/dnssec_maint_tool

Need someone to host a signed zone as a primary or secondary server? Willing to host signed zones for others? Go to:
http://dnssec-deployment.org/zones/

What You Can Do

Prepare: **Zone operators should understand the requirements and evaluate their environment against those requirements to determine what changes may be needed.**

Download: **Software is readily available for servers, clients and many operational tools. Review the "DNSSEC Resources" section to see what DNSSEC-aware software can do for you.**

Pilot: **Tests of the software environment are needed, including development and testing of internal procedures, integration with existing environments, and fine-tuning operations through monitoring and evaluation.**

Educate: **Train operations staff and customer service representatives, and communicate new DNSSEC-compliant services to customers.**

Deploy: **Make new DNSSEC-compliant services available to users and customers.**

Find out more about the DNSSEC Deployment Initiative and Early Adopter Experiences at:
http://dnssec-deployment.org