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. See what DNSSEC-aware software can do for you:

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

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

UNBOUND resolver prototype:
http://www.rfc.se/unbound/

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

Test: Tests of the software environment are needed, including development and testing of internal procedures and integration with existing environments.

Educate: Communicate new DNSSEC-compliant services to customers.

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

Find out more at
http://dnssec-deployment.org

DNSSEC Resources

Tools, Information, Links

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

DNSSEC Tools:
http://www.dnssec-tools.org

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

Early Adopters

RIPE NCC:
http://www.ripe.net/reverse/dnssec/

Sweden:
http://www.iis.se/english/dinadomaner/dnssec.shtml?lang=en

Public Internet Registry:
http://www.pir.org/Strengthening/DNSSec.aspx

VeriSign:
http://www.verisign.com/research/DNS_Research/index.html

Germany:
http://www.denic.de/en/domains/dnssec/

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/

A Domain Name System Security
Deployment Initiative Workshop
http://dnssec-deployment.org

200703-003-A4

DNSSEC for TLDs: Experience from Sweden and Bulgaria

Improving the security of the Internet's naming infrastructure

ICANN

28 March 2007
3:30pm – 6:00pm
Jade 1 & 2

Lisbon, Portugal

DNS Security

Most users trust the Internet's system of domain names and expect to be directed reliably to the website they've entered in a browser. Unfortunately, that's not always the case. Attackers can disrupt the domain name system (DNS) by forging network packets or gaining illicit access to servers on the network to corrupt or destroy information. The ability to redirect users to other domains leaves openings for fraud in electronic commerce and the risk of a terrorist attacks on the Internet infrastructure.

Securing the domain name system is an important part of securing the Internet infrastructure for the challenges it faces in the next century. Serious DNS attacks are a reality today—it's estimated that 10 percent of servers in the network are vulnerable to DNS attacks. Users cannot prevent or detect these attacks, so security measures at the infrastructure level are needed. Security measures are underway in a global, cooperative effort to help DNS perform as people expect it to – in a trustworthy manner.

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.

How It Protects

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 be used to trace the addresses used for web and email servers back to the bona fide owner of the domain. 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.

Workshop Agenda

Welcome
Steve Crocker, Co-Chair DNSSEC Deployment Initiative

DNSSEC as a Service in Sweden

Swedish Strategy for Safer Internet
Jörgen Samuelsson, Head of Section Ministry of Enterprise, Energy and Communications

Task and Challenges for the ccTLD
Staffan Hagnell, Head of R&D .SE

Resolving DNSSEC for Broadband Customers
Mats Dufberg, Senior Engineer TeliaSonera

Why DNSSEC?
Kjell Rydjer, Senior Security Architect Swedbank/CIO Strategy and Architecture Strategic responsible for the IT Security and Communication in Swedbank Group

DNSSEC within the Government
Anders Rafting, the Swedish National Post and Telecom Agency

The Mission for Registrars, DNS-Operators, Applications and Users
Staffan Hagnell, .SE

DNSSEC IN BULGARIA
Daniel Kalchev, Technical Director, Register.BG

Questions, Answers and Discussion
Steve Crocker