Improving the security of the Internet's naming infrastructure

Monday, 11 February 20087
11:00 – 13:00
Jaipur Room

ICANN 31 | New Delhi, India

DNSSEC in the Field

Agenda

Welcome
Steve Crocker
Co-Chair DNSSEC Deployment Initiative

Surveys and Trust Anchor Repositories

Two surveys of signed zones are conducted regularly. We present their results, including the reasons they report somewhat different numbers. We also focus on zones which are signed below unsigned parents, thereby requiring a publication process.

- Surveys of IKS-Jena's Lutz Donnerhacke and UCLA's SecSpider project
- The DLV Trust Anchor Repository – Suzanne Woolf, Internet Systems Consortium

One Year of Operational Experiences
Staffan Hagnell

DNSSEC Position Statement from SSAC
Steve Crocker, SSAC Chair

Questions, Answers, and Discussion
Steve Crocker

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/

DNS Security

Most users trust the Internet's system of domain names and expect to reliably reach the destination they've entered in a web browser, email client, or other application. 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 today and in the future. 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 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.

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