Infrastructure Security DNS and Routing

Status and Update

Sandra Murphy

sandy@sparta.com, sandy@tislabs.com



DNSSEC Is Live!

- RIPE has signed all IPv4 reverse and a select set of forward zones:
 - http://www.ripe.net/projects/disi/keys/
- And will create secure delegations:
 - https://www.ripe.net/rs/reverse/dnssec/registryprocedure.html
- NIC-SE has signed .se and will create secure delegations:
 - http://dnssec.nic.se/

DNSSEC Deployment Initiative

- Open working group focusing on deployment issues - active mailing list, regular telecons
- Organizes DNSSEC Workshops at conferences around the world (ICANN, Internet2, Joint Techs, APRICOT).
- Web site for news, charts deployment progress, provides support for deployments, and outreach to those considering DNSSEC:
 - http://www.dnssec-deployment.org/

Working Group

DNSSEC Deployment Initiative











http://www.dnssec-deployment.org/





Events/Archives





Home

DNSSEC Deployment Initiative

DNSSEC Deployment Initiative

Applications

Technology

Monday, February 13, 2006

News

Posted: 12 Jan 2006 RIPE NCC Signs Reverse Delegation Zones

Posted: 19 Dec 2005 **DNSSEC Hedges Against** Degrading Trust in SHA-1

Posted: 13 Dec 2005 IETF standard for the registrar-to-registry communications for DNSSEC published (RFC 4310)

News Archive

New on the Site

- DNSSEC Workshop - The Registrars' View - ICANN Vancouver [proceedings]

- Measuring the resource requirements of DNSSEC

Welcome

Outreach/Adoption

This is the website for the DNSSEC Deployment Initiative, which is a self-organizing, open effort made up of anyone active in deploying DNSSEC. The initiative includes an expert working group holding frequent discussions. The site publishes news, charts deployment progress, provides support for those actively engaged in deploying the protocol, and offers outreach to those considering DNSSEC.

Operational Guidelines

DNSSEC (a shorthand for DNS security extensions), is an addition to the DNS that allows enabled systems to detect compromised domain name information. It does not stop or prevent attack, but it allows the systems to identify DNS data that is untrustworthy.

RFC 3833 describes threats and attacks on the domain name system, and this page collects information on actual attacks and measurements related to risk. The extension for DNSSEC is specified primarily in RFC 4033, RFC 4034 and RFC 4035. An excellent introduction and explanation of DNSSEC is provided by this document. Another key piece for deployment, the Extensible Provisioning Protocol (EPP) application for registrar-to-registry communication of DNSSEC information, is specified in RFC 4310.

For extensive technical background information, please visit the DNSSEC - DNS Security Extensions site. This is a great site with important references to the development of the protocol, configuration guides, technical papers and so on.

Other Sites to Visit:

DNSSEC Project at NIST

NLnet Labs DNSSEC

DNSSEC Deployment at RIPE

DNSSEC at .SE

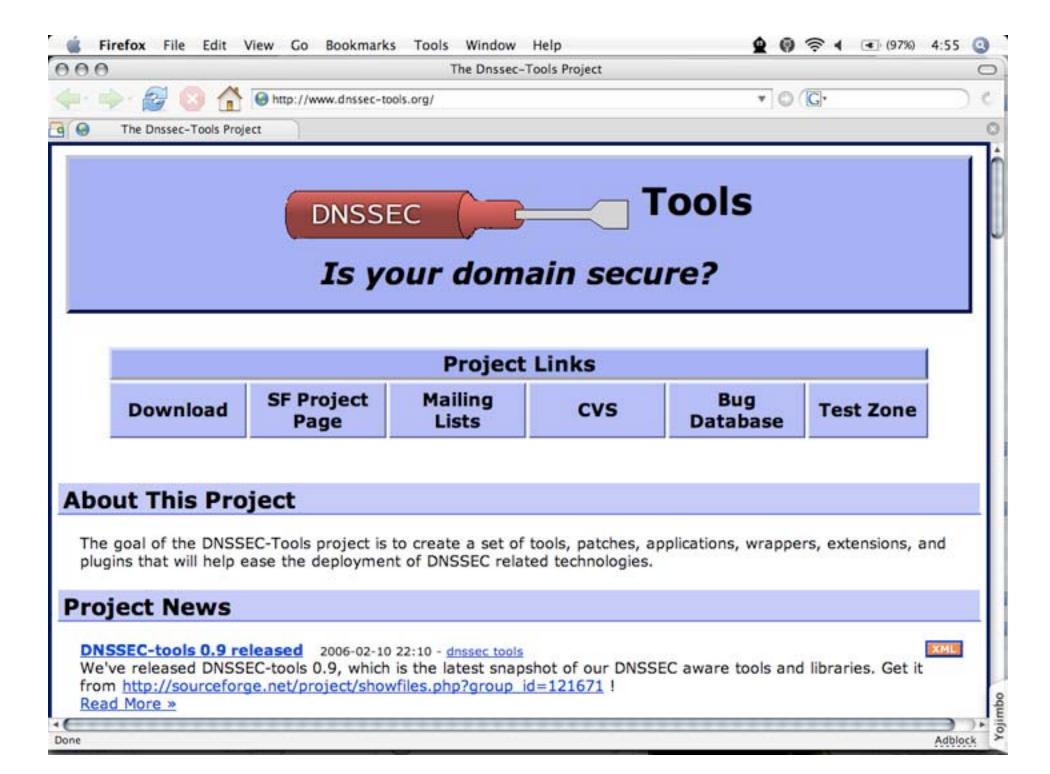
The DNSSEC Tools Project at Sparta

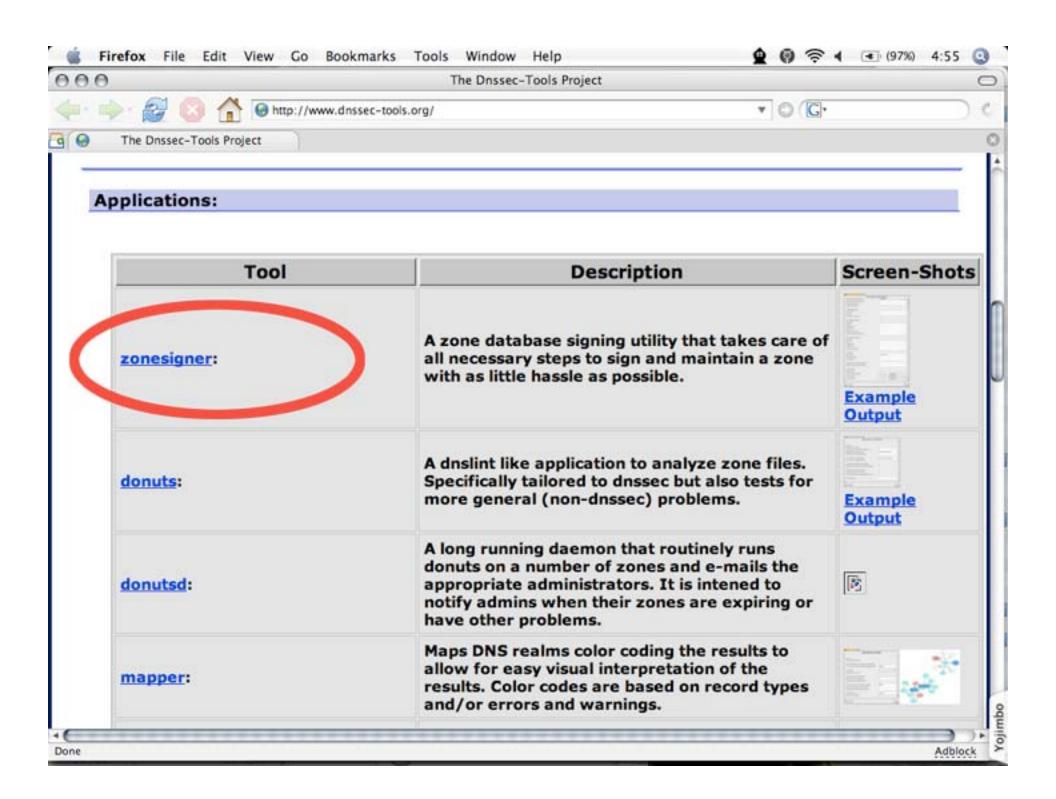


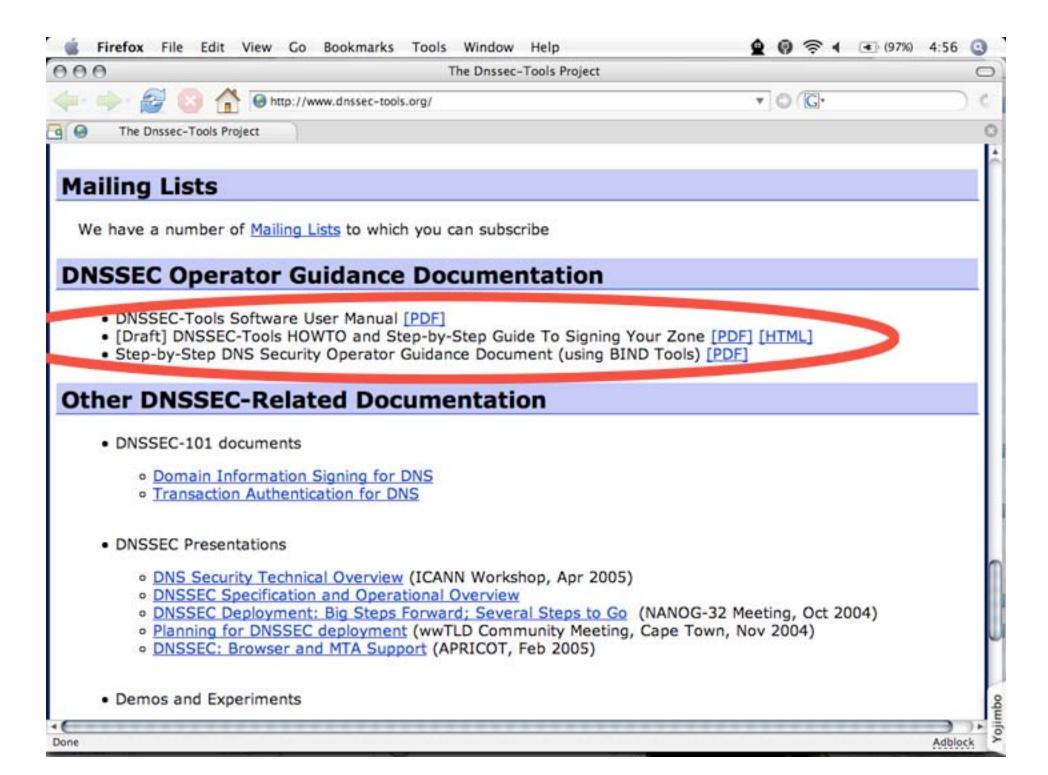
Search

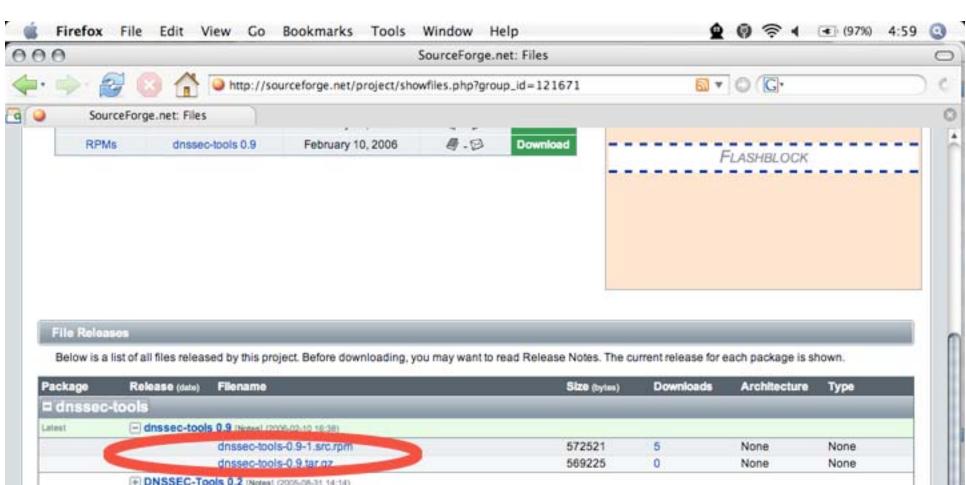
DNSSEC-Tools Project

- Create a set of tools, patches, applications, wrappers, extensions, and plugins to ease DNSSEC Deployment:
 - http://www.dnssec-tools.org/
- Current release is v0.9 from 02/10/2006
- Also have released a modified Firefox 1.5 RPM that uses DNSSEC-Tools to validate signed zones.









Miller Street, and	Children and Children Children and Children	(hetetelectrical)	The Bud Add Add Add Add Add Add Add Add Add A	effentie de tetrate de la constitución de la consti	Del. Land
□ dnssec	-tools				
Latest	dnssec-tools 0.9 (Novemb (2005)22-10 18:38)				
	dnssec-tools-0.9-1.src.rpm	572521	5	None	None
	dnssec-tools-0.9 tar.gz	569225	0	None	None
	→ DNSSEC-Tools 0.2 [Notes] (2005-08-31 14:14).				
£1.	+ dnssec-tools 0.1 [Notes] (2005-05-08 11:41)				
□ RPMs					
Latest	- dnssec-tools 0.9 [Notes] (2006-02-10 16:38)				
	dnssec-tools-0.9-1.fo4.i386.rpm	120998	1	None	None
	dnssec-tools-debuginfo-0.9-1.fc4.i386.rpm	243304	0	None	None
	dnssec-tools-libs-0.9-1.fc4,i386.rpm	77297	1	None	None
	dnssec-tools-libs-devel-0.9-1.fc4.i386.rpm	98974	0	None	None
	0.4.fc4.j386.rpm	67283	1	None	None
	Firefox 1.5 with dnssec [Notes] (2006-02-06 16:15)				
	firefox-1.5-dnssec.1.fc4.i386.rpm	11968051	6	None	None
	firefox-1.5-dnsseq.1 src.rpm	41540976	0	None	None
Totals:	5 11	56268781	217		

Securing the Routing Infrastructure

- Important problem, but no traction on deployable solutions
- Three workshops have been held with a wide net of the interested parties
 - Operators (ISPs, access and content providers), vendors, security geeks
 - DHS hosted, anxious to find and facilitate a solution
 - http://www.hsarpacyber.com/public/spri/

Operators' Emphasis

- A strong call from the operators for an authenticated list of authorized prefix originations (accurate, complete, secure..)
 - Useful in responding to customer requests to route a prefix
 - Useful in debugging routing difficulties
 - Useful in building filters
 - Necessary first step of any solution for BGP route verification

New ARIN Policy Suggestion

Recommendation

 New field in address templates (direct and sub delegations) for list of permitted ASs

Benefits

- Inherits self-discipline of completing the form (IRR entries aren't always done)
- Inherits scrutiny of ARIN process on creation
- ARIN is authority for who is allocated prefixes
- Any IRR would have to check prefix with RIR

Authentication and Currency in IRRs

Authenticating IRR objects

- RIR run IRRs have internal access to authentication for prefix holders
- Non-RIR run IRRs would have to find a way to get that authentication from the RIR
 - Same is true for RIR IRR objects referring to nonmember resources
- Currency for IRR objects
 - Reclaimed resources have to result in IRR purges
 - Why not a TTL in IRR objects?