DNSSEC Deployment: Early Lessons Learned

Scott Rose
NIST
scottr@nist.gov
Summer JointTechs Meeting
Lincoln, NE
July 21-23, 2008
Outline

• Overview of NIST zones
• How DNSSEC has affected infrastructure
• Trends seen in other deployments
• Things to consider when deploying DNSSEC on your campus network
Several delegations each managed locally
nist.gov DNS Now

Size of nist.gov zone: 22,000 RRs ~19MB memory in BIND when signed
What Happened?

• FISMA and other security regulations
  – DNSSEC is part of FISMA, but not sole driving force
  – Both top-down and bottom-up

• Cost/operational issues

• Those that remain do so for several reasons
  – experimental systems going up/down
  – operational/geographic issues (Boulder campus)
  – stubborn pride
DNSSEC Deployment at NIST Campus

- Started at divisional level (antd.nist.gov)
- So far only the authoritative side
  - i.e. Zone signing and TSIG for zone transfers
- Administration is still largely informal
  - TSIG and DS RRs transferred via email
  - Tools mostly home brewed: script wrappers around BIND tools
DNSSEC Deployment at NIST: Lessons Learned

• TSIG key exchange
  – email easiest, other methods may be more secure but prone to errors

• Key generation (BIND tools and scripts)
  – Need a good source of entropy or process slows down

• Zone Signing
  – Tools help. Just using BIND tools sometimes results in errors and delays in updating zone
  – Time becomes important.
DNSSEC Deployment at NIST: Lessons Learned

- Automation scripts helpful
  - best used for zones that do not change
- Where to we send our DS RRss?
  - Not just for nist.gov but also for .org/net delegations
  - DS RR better than uploading DNSKEY RRset
DNSSEC Deployment: Issues from Other Deployments

• Content Management and signing
  – Where/how to integrate signing tool into process
  – Using dynamic update to update zone data complicates matter
    • Signing keys have to be on server

• What about Windows deployments?

• How do I know I will meet security audits?
  – Do what by when?

• What about the resolution/validation side?
Cavalry on the Way?

- OMB to issue memo on DNSSEC
  - mentioned by Karen Evens (OMB) but not released yet
  - direction for .gov?
- Revisions of relevant NIST publications:
  - SP 800-81, SP 800-57 Part 3, SP 800-53
- Trust Anchor Repositories
  - Whitepaper on technical issues
  - IANA, RIPE NCC all working on some sort of TAR
  - There is also DLV
- PIR plan for DNSSEC deployment in .org
Cavalry on the Way?

• DNSSEC and Tools
  – companies starting to view DNSSEC as possible market for tools HSMs, and appliances
    • Help with zones that rely on dynamic update?
• We have another validating resolver – Unbound
  – NLNet Labs (nlnetlabs.nl)
• Microsoft – still moving forward on DNSSEC
• Training classes
  – RIPE NCC, NIST and others
So What to Take Away when Deploying at Home

• Biggest issue: Content Management
  – Every deployment is unique.
  – Redesign the zone/domain may be required

• Don't sign in a vacuum
  – Work with delegations and parent (if possible)
  – Work out how to exchange TSIG keys/DS RRs

• Help is out there
  – Learn from others' mistakes/successes
  – Training
  – Guidance documents
  – Pilot testbeds (SNIP)
Resources

• Secure Naming Infrastructure Pilot (SNIP)
  – Pilot testbed, training announcements, resources
  – http://www.dnsops.gov/

• DNSSEC Deployment Initiative
  – News, announcements, links to tools and guides
  – http://www.dnssec-deployment.org/