DNSSEC Guidance Document

R. Kevin Oberman

July 22, 2009

Summer 2009 ESCC
IUPUI
Indianapolis, Indiana

ESnet
Energy Sciences Network

Supporting Advanced Scientific Computing Research • Basic Energy Sciences • Biological and Environmental Research • Fusion Energy Sciences • High Energy Physics • Nuclear Physics

Berkeley Lab

U.S. Department of Energy | Office of Science

Overview

OMB has mandated DNSSEC for .gov by the end of 2009. Most ESnet sites have zones in .gov, so will be implementing DNSSEC soon.

This document provides general guidance and not specific implementation details.

DNSSEC Operation

- DNSSEC uses public key cryptography
  - Similar to SSH
- DNSSEC uses an anchored trust system
  - NOT PKI! No cetificates
- Trust must start at the root and follow the DNS heirarchy
- You generate key pairs and sign your data
- You make keys available to your parent

When to sign

- Now, now, or now. Take your pick.
  - Signing has NO external impact!
  - Publishing keys DOES have impact!
- This is the perfect time to test and experiment as you are free to mess it up
  - Once you publish keys, you really don't want to mess up!

What to sign

- Forward zones are the big win
  - Reverse zone signing has value
  - Less impact than the forward zones
- You may not want to sign some reverse zones
- Maybe not forward zones, either
  - Cases for not signing forward zones are few and far between

Signing

- Signing usually involves to keys
  - One for signing zone data (ZSK)
  - One for signing keys passed to parent (KSK)
- Keys need to be changed (rolled) regularly
- Signatures (not keys) expire
  - Expired keys means no DNS availability

Signing policy

- Use two active keys (for both ZSK and KSK)
  - Data is signed by two newest keys
- Sign at short intervals compared to expiration times
  - Provides a buffer to deal with failures
  - ESnet is signing evey 12 hour
  - ESnet has a one week signature life

Signing systems

- Do it yourself
  - Cheap
  - Not easy
  - Will get MUCH easier

Signing systems (2)

- Free tools
  - DNSSEC-tools
    - Suite of tools that can be used to create a system
  - OpenDNSSEC
    - Turnkey software
    - Support HSMs
    - Not yet completed
  - BIND
    - Limited but will be much enhanced in 9.7

Signing systems (3)

- Two known to exist
  - SECURE64
  - Xelerance
- Others MAY be close
  - Infoblox
  - Bluecat Systems

Certification

- No current requirement for certification
  - This may change as OMB tightens requirements
- Relevent standard is FIPS140-2
- No currently available products are FIPS certified
  - Secure64 has submitted audit results to NIST

Operational Concerns

- You need at least two people able to work with your system
- You need a backup system
- You need an repair/replacement time of less than the shortest possible interval between signing and signature expiration

Testing and developemnt

- Start testing ASAP!
  - Once you go live with published keys, testing is limited
  - Set up a validating server to allow testing of signed data
  - Do lots of testing