DNSSEC Implementation at ESnet

R. Kevin Oberman
Sr. Network Engineer
February 2, 2010
Why ESnet is Signing

• While not covered by the OMB mandate, ESnet supports several organizations which are required to sign

• ESnet needs experience with DNSSEC to support these organizations effectively

• Future mandates may cover ESnet
How ESnet is Signing

• Secure64 Secure Signer appliance
  – Transfers zones from existing master
  – Public DNS Servers transfer data from the appliance

• Compliant with all SP800-81 requirements
  – Current release does not support SHA256

• FIPS 140-2 Level3
Systemic Problems

- .net is not signed
- .org is signed
  - Registrar will not accept SEPs
  - .gov will accept DS records
- Only reasonable path is DLV
  - Operated by ISC (BIND maintainer)
  - Well supported by most DNSSEC capable servers
Testing and debugging

• Limited tools available
  – dnscheck.iis.se
    • Web based
    • Fairly thorough
    • Can be installed locally (Requires perl)
  – drill – dig(1) look-alike that understands DNSSEC better
Progress and Problems

- Signer appliances installed end of July
- Initial zones loaded and signed early August
  - V2 code had several problems
    - Signer code worked fine
    - TCP stack had issues
    - Did not work properly with our master
  - V3.1.6 solved last problems
• Confirmed full operational capabilities in early December
• All public servers started serving signed data December 18, 2010
• Tested verification with LBNL in January
Status today

• Will start publishing SEPs in the DLV in next week
• Holding KSK roll until April
• Temporarily signing for one site
• Will install backup signer box in New York this month