DNSSEC Update

R. Kevin Oberman
ESnet

February 5, 2009

.gov Now Signed!

- .gov formally signed Feb. 1
  - Not yet accepting delegated keys
  - Will start doing so in a few days

Time to sign

- With signed .gov, it is time for those in .gov space to start signing
  - Be sure that you are ready
    - Don’t rush
    - Test before officially signing

How to Sign

- http://www.dnssec-tools.org
  - Work done by Sparta under contract to the US Government
  - Tools are open source and free
  - Allow fairly easy implementation of most DNSSEC requirements
- Signing appliance
  - Easiest operation
  - Least likely to fail

Use BIND-9.6.0-P1 or later

- Supports NSEC3
  - NSEC3 prevents zone enumeration
  - Required to 'hide' zone data
    - Prevents effective zone transfer
- Supports 'automatic' key update to parent
  - Greatly simplifies key management

Key Issues

- Two ‘types’ of keys
  - Zone signing keys (ZSKs) sign RRsets in zone files
  - Key signing keys (KSKs) sign the ZSKs
- All keys use symmetric public keys much like ssh
- Data may be signed by multiple keys

Key Management

- Zone signing key must be changed monthly
- Key signing keys must be changed annually
- Valid public key must ALWAYS be available for current and cached data
  - Watch TTLs—long cache life complicates emergency key changes
  - TTLs should probably be no longer than a few hours

Three Key Shuffle

- Keys A, B, and C
- Data signed with A and B
- To roll keys:
  - Generate new key pair (C)
  - Sign data with B and C
- Keeps each key active for two cycles
- All cached data always signed with active key

No Room for Error!

- Data not signed by valid key will not validate
- Queries for your data will fail on validating servers
  - Your zone will ‘disappear’ from the Internet
  - Your users will be very unhappy!

No Key Revocation!

- Keys may be withdrawn, but not revoked
- New key can be put in place very quickly
  - Cached data will not be valid if no valid key is in place
  - Keep TTLs short

The Clock is Ticking

- OMB requires that zones immediately under .gov be signed by the end of 2009
- You need to start working on a signing solution NOW!