DNSSEC Implementation

R. Kevin Oberman
ESnet
Berkeley Lab

25-Enero-2009

NANOG45-Santo Domingo, DR

Key Generation is Easy

- One quick command
  - Yes, it is a long, odd looking command
  - See NIST SP800-81 !

Signing Data is Easy

- Zone Signing requires a single command
- Takes just seconds
- Can be automated fairly easily for DDNS
  - See NIST SP800-81!
  - http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

Validating is Easy

- Just turn it on in BIND
- Provide pointer for DLV
  - See NIST SP800-81

So, what's the big deal?

Details, Details, Details

- What if your DNS management tools don't support DNSSEC?
- How do you change keys?
- How do you revoke a key?
- How do you transfer the keys to your parent?
- How do you deal with an unsigned parent
  - .com, .edu, .gov, .net, etc.
  - Root is unsigned, too!

Key Terms

- All keys use public key technology
- Zone signing keys (ZSKs) sign the actual data
- Key signing keys (KSKs) sign the ZSKs
  - KSKs must be transferred to parent
- RRsets each require a signature
- RRsets eash require an NSEC record
- NSEC records used for verified non-existance

Key Update

- If your data signatures don't validate, you're down!!
  - Zone signing keys should have a short life
  - You will need to re-sign data regularly
  - You need to update parents
  - **You can't make a mistake!**

Solutions?

- DNSSEC Appliances
  - Act as proxies
  - Automate signing to avoid errors
  - Automate key signing
  - Protect keys

Solutions?

- DNSSEC-Tools (dnssec-tools.org)
  - Provides scripts for most common DNSSES ops
  - Actively under development to incorporate new standards and software capabilities
  - Mostly a product of SPARTA (Thanks!)

- Get the damned root signed!
  - This is a political issue today
  - If you can provide any infuence on DOC, please do