DNS Security:
A Trusted Naming Infrastructure for the Internet
http://www-x.antd.nist.gov/dnssec/

DNS – User’s Interface to Internet

- Importance of DNS Names
  - URI part of our language now
  - dougm@nist.gov, www.nist.gov., ibm.com
- Complexity of DNS-System
  - ~50-100 queries to load a news.ecommerce web page.
  - Dynamic DNS resolution
    - CDNs, load redirections.

Other Forms of DNS Attacks

Other Forms of DNS Attacks

- Recursive / Caching Server
- End-user
- Man in the Middle
- Zone Servers
- Forged data
- Actual <time.nist.gov A 192.43.244.18>
- But how can you validate this?

DNSSEC Chain of Trust

DNSSEC Chain of Trust

- “.” – DNS root.
- KSK
- ZSK
- Trust Anchors installed on client resolvers.
- # of Trust Anchors?
  - Top Level: 1 trust anchor minimum
  - 2nd Level (TLD): 100’s possible
  - 3rd Level: millions likely

DNSSEC Deployment Guidance

DNSSEC Deployment Guidance

- Secure DNS Deployment Guide
  - NIST Special Publication 800-81
  - Deals with DNS Security, not just DNSSEC
  - Technical deployment guidance for enterprise DNS administrators and security officers.
  - Provides both information for robust configuration of traditional DNS services and deployment / operational guidance for DNSSEC.
  - Provides cookbook configuration examples for commonly used DNS servers.
- DNSSEC Key Management Guides
  - NIST Special Publication 800-57 Parts 1,2,3
  - Key / Algorithm parameters for DNSSEC
  - Puts DNSSEC in context of general USG requirements for key management and use.

DNSSEC Tools, Tests & Testbeds

DNSSEC Tools, Tests & Testbeds

- Open Source Test Tools
  - NIST Zone Integrity Tester
  - Load generation and perf tools.
  - Performance analysis reports.
- Secure Naming Infrastructure Pilot (SNIP)
  - USG / Industry tested to experiment with DNSSEC technologies.
  - Practice new zone administration processes.
  - Pilot USG .gov TLD key management processes.

Starting From the Top: .gov & root

Starting From the Top: .gov & root

- Deployment at the .gov gTLD.
  - Feb 2009 - First global TLD to operationally deploy DNSSEC
    - NSEC3 signed, 2048bit keys, trust anchor @ time.nist.gov.
    - Dotgov.gov registry is up & operational
    - Accepting secure delegations from secondary’s.
    - POC authentication and notification functions.
    - Manual and automated key rollover functions.
    - Monitoring and diagnostics for USG signed zones.
    - Prepared to accept other .gov secure delegations (states, etc.)
  - Registry Interface integrated with SNIP
- Deployment at the global DNS root.
  - NIST & NTIA developing technical plans to sign the root.
  - Global root signed in 2010.