NIST
National Institute of
Standards and Technology

INFORMATION
TECHNOLOGY
LABORATORY

DNSSEC in .gov: What is happening, and what you need to do.

Scott Rose

NIST

scottr@nist.gov

July 27th 2010

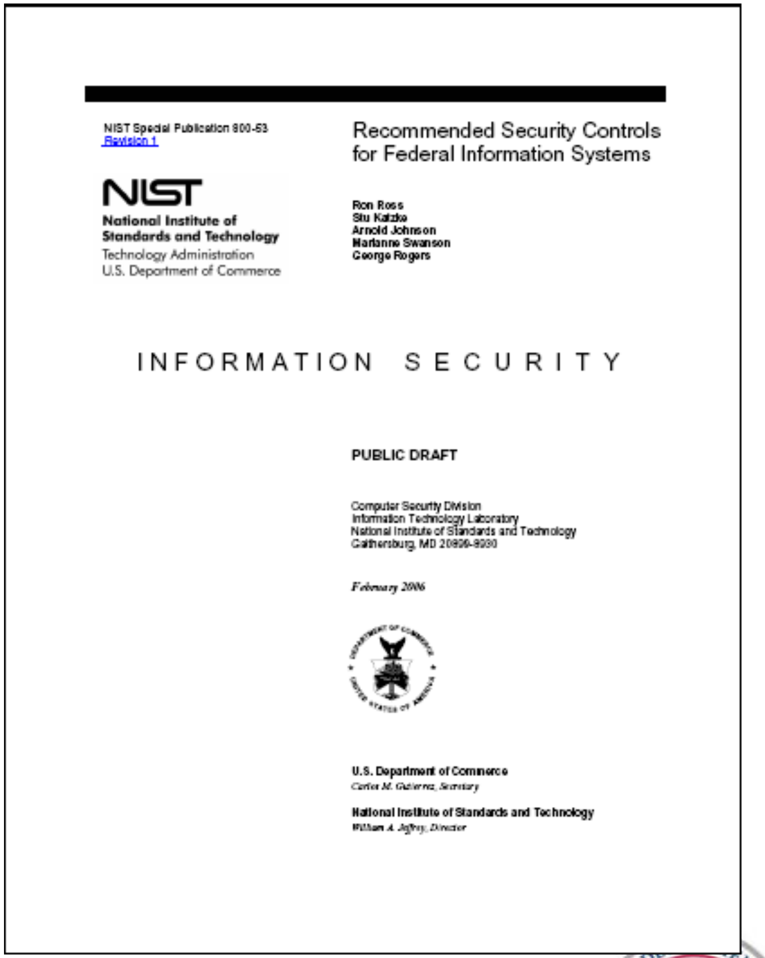
Cyber and Network Security Program

History: Deployment Drivers

- Office of Management and Budget (OMB) issues Memo (M-08-23), August 2008
  - Issued order to sign the .gov TLD by Dec. 08 (actually signed Jan. 09)
  - All 2nd level, external facing zones signed by Dec. 09
- Federal Information Security Management Act (FISMA)
  - Security audit for all US Federal IT systems
  - Audit controls covering DNSSEC included in Dec. 2007 (expanded in latest revision in 2009)
    - By law, takes effect 12 months after publication (here, August 2010)

DNSSEC and FISMA

- **Putting the FISMA Puzzle Together.**
- **FIPS-200** *Minimum Security Requirements for Federal Information Systems*
  - Points to NIST-880-53 *Recommended Security Controls for Federal Information Systems* for technical controls to meet these requirements.
- **NIST-800-53r3**
  - Published Aug 2009
  - Defines DNS security controls
  - Cites NIST-800-81 used as reference.
- **NIST-800-53A**
  - Provides guidance for auditors on controls
- **Promulgation – closing the loop.**
  - Final FIPS-200 published March 2006.
    - Effective immediately, 1 year for compliance according to FISMA
    - Most FISMA C&A audits occur every 3 years.



NIST Special Publication 800-53
Revision 1

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommended Security Controls
for Federal Information Systems

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
George Rogers

INFORMATION SECURITY

PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William A. Jeffrey, Director

DNS Related Controls in SP800-53r3

- SC-8 Transmission Integrity
  - For Moderate and High
  - Use of Transaction Authentication/Integrity methods for server-server transactions
  - TSIG for zone transfers/dynamic update (or similar)
- SC-20 Secure Name/Address Resolution Service (Authoritative Source)
  - For Low, Moderate and High (i.e. Everyone)
  - DNSSEC signing of *all* zone data
    - Internal and external zones, at all levels of the DNS tree.
    - Much more extensive than the OMB mandate
  - Reference: NIST SP800-81

Cyber and Network Security Program

DNS Related Controls in SP800-53r3

- SC-21 Secure Name/Address Revolution Service (Recursive or Caching Resolver)
  - For High category only (Expect it to go down in future revisions!)
  - Recursive servers (Primary and Secondary) must be able to validate DNSSEC signed responses.
  - NIST SP800-81 referenced
- SC-22 Architecture and Provisioning for Name/Address Resolution Service
  - Moderate and High currently (may also go down in future revisions)
  - Non-DNSSEC control
  - addresses other best security practices for DNS deployment and operation

NIST SP800-57 Recommendations for Key Management

- 3 part guide for key management within the USG
- Part 3: "Where the rubber meets the road"
  - Broken down by protocol
  - Gives guide for procurement and administrators when looking to configure software packages
    - Base requirements for crypto support, key size, key life cycle issues, etc.
    - Migration from weaker to stronger hash algorithms, crypto algorithms, key sizes over time.
- DNSSEC is one of the protocols
  - Material for section taken from SP800-81 and best common practices guides

Current State of Deployment

- OMB Deadline passed, FISMA still to take affect
  - Not a huge success, most agencies missed deadline.
  - Roughly 280 out of 1400+ delegations signed
    - Exact numbers hard to obtain
    - Not including US State/local government delegations which are not required to deploy, but some have.
  - Still see push-back or lack of knowledge about deployment
- Not a lot of validation yet (not required by policy)
  - Unknown problems may lurk? (firewall/MTU issues)
- Have not heard of provisioning/resource problems
  - No major spike in TCP requests

Lessons Learned

- Administrator education should be a major priority during deployment.
  - Admin error the cause of most problems
  - Give administrators time to plan and clear policy guidance about what they need to do.
  - Know who to contact when mistakes occur
  - Establish a help desk/support network to resolve issues.
- For large domains: establish a procedure for your delegations to upload key material to the parent zone

Lessons Learned

- DNSSEC centric crypto policy is important (DNSSEC is not a PKI)
  - US Federal key policy aimed at PKI certificates (i.e. large, long lived keys), not DNSSEC.
    - causes large response sizes and problems in some routers/firewalls
    - Special guidance developed for DNSSEC to continue to allow smaller keys for a period of time (until 2015)
- Look at your other network components for hidden dangers
  - Old routers/switches or firewalls may drop large DNSSEC responses
    - 1500 bytes a reasonable MTU setting
  - Firewall rules may need changed (UDP & TCP port 53)

Lesson Learned: Interacting with .gov

- GSA (sole registrar) web portal: http://www.dotgov.gov/
  - Requires registration login/password (up to 5 POC's per registration)
- Uploading DNSSEC key material
  - upload keyset file (plaintext file)
    - Problems: Only certain formats accepted (soon to fix?)
    - Tip: system checks all name servers for the key – so make sure your signed zone is published first, then upload the key.
    - Tip: keys must conform to Federal policy (2048 bit RSA/SHA-1 or RSA/SHA-256)
- Has optional monitor service for automated key rollovers
  - Either way: old DS RR's should stay around for 3 days, then are removed from the zone.

What to Expect in the Future

- The Root zone is signed
  - The .gov TLD DS will appear soon
  - More and more ISP's and enterprises will be validating
  - What you may see:
    - More queries (for keys), so (slightly) more bandwidth used
    - Reports that older firewalls/routers/switches dropping DNS replies (need to be replaced)
    - If you mess up...you will "disappear" off the net!
- DNSSEC deployment in .gov merged with the Trusted Internet Connection (TIC) project
  - Same team (TIC deployment) also tasked with monitoring/ measuring deployment

Deployment Aids

- NIST Special Publication 800-81(r1): Secure Domain Name System (DNS) Deployment Guide
  - Contains recommendations and DNSSEC specific Federal cryptographic key requirements.
  - http://csrc.nist.gov/
- Secure Naming Infrastructure Pilot (SNIP)
  - Distributed testbed for agency use
    - http://www.dnsops.gov/
- DHS funded blog/news site
  - http://www.dnssec-deployment.org/