NIST
National Institute of
Standards and Technology

INFORMATION
TECHNOLOGY
LABORATORY

DNS Security Extensions (DNSSEC) Briefing

Created by the DNSSEC-Deployment Initiative

Modified and Presented by Scott Rose, NIST

scottr@nist.gov

June 3, 2009

Cyber and Network Security Program

DNSSEC

To put DNS vulnerabilities in context…

- Central role of DNS
  - the Internet’s address system
- Why DNS is at risk
- DNSSEC: The Security Extensions
- DNSSEC and FISMA
- NIST provided guidance and tools
- Deployment Progress and Lessons Learned

About DNS

- Domain Name System (DNS)
- Worldwide database, widest deployed standards-based name system
- Essential component of Internet
  - Robust even in the presence of some errors
  - Often the first part of any Internet transaction
- Due to lightweight, distributed nature, attacks very difficult to detect

Why DNS Is At Risk

- Designed in 1980s, different threat model
- Optimized for fast query/response times, not for security; trust implied and expected
- DNS threats first identified in early 1990s
- Not designed for:
  - wide public use
  - current functions
  - current scope: .com and .net today capable of handling 400 billion DNS queries every day

Why DNS Is At Risk: Threats and Attacks

- Attacks via and against DNS infrastructure are increasing
- DNS seen as critical weakness in National Strategy to Secure Cyberspace (2003)
- Financial/large enterprises see major increases in online attacks for fraudulent purposes
  - Consumer confidence decreasing
- Tools available: no learning curve required

Most Recent Attack

- Rapid, widespread and resilient
- Reduces time required to poison recursive name server's cache
- All known name server implementations are affected
  - Some more than others (took < 10s to poison the cache)
  - Most implementations patched; now as easy/difficult to poison as any other implementation
- Even patched software vulnerable
  - cache poisoning attempt possible in < 10 hours

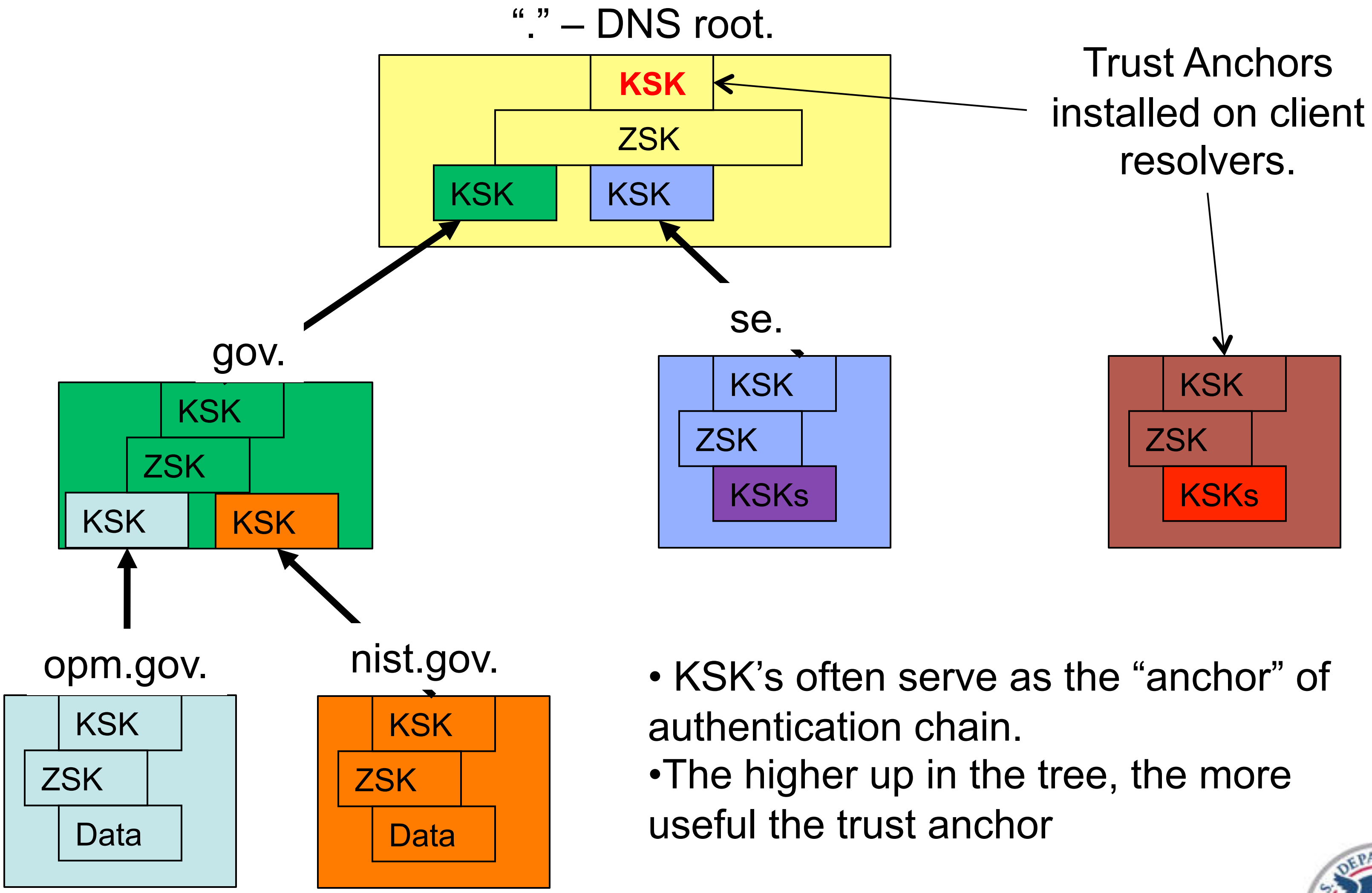
DNS Security Extensions (DNSSEC)

- Internet Systems Consortium: DNSSEC “only full solution” to recent attacks
- Considered more viable long-term solution, compared to patches
- DNSSEC provides users with technical basis for verifying DNS answers from name servers
  - Uses public/private key cryptography
  - Adds required data to Zone
  - From user perspective, DNSSEC does not change zone content

What DNSSEC Provides

- Cryptographic signatures in the DNS
- Integrates with existing server infrastructure and user clients
- Assures integrity of results returned from DNS queries:
  - Users can validate source authenticity and data integrity
- Checks chain of signatures up to root
  - Protects against tampering in caches, during transmission
- Not provided: message encryption, security for denial-of-service attacks

DNSSEC Chain of Trust



- KSK's often serve as the "anchor" of authentication chain.
- The higher up in the tree, the more useful the trust anchor

Drawbacks of DNS Security

- Increased complexity
  - Extra queries to create chain of trust, resolvers able to verify digital signatures
  - Key management now a factor in DNS operations
- Increased zone database size
  - Contain more records, doubling or tripling size of DNS zone database
    - example: nist.gov (22k RRs): 9.5 MB usigned, 19 MB signed.
- Increased interaction between delegations
  - To secure delegations to sub-zones

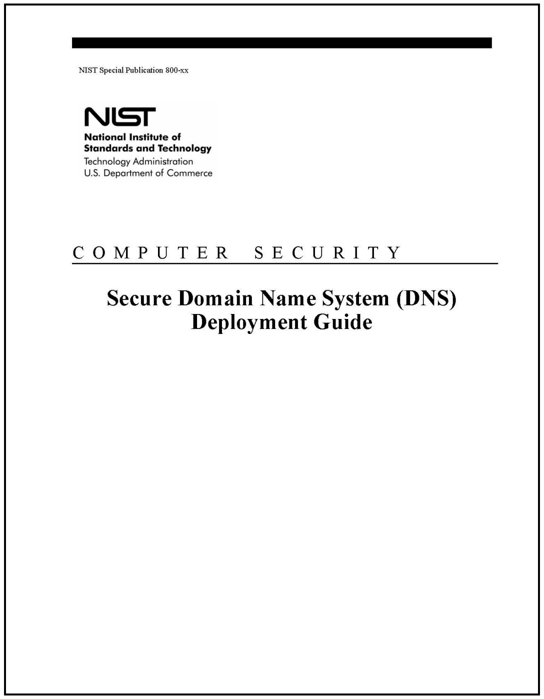
DNSSEC Deployment

- US Department of Homeland Security Science & Technology Directorate programs
- DHS cannot secure Internet by itself
  - Taking leadership role, facilitating public-private partnerships (industry and government)
- Outside of the USG:
  - Several ccTLD's currently signed
  - .org in process
  - Verisign announced .com/net to be signed by 2011

DNSSEC Guidance

- **Secure DNS Guidance Documents**
  - NIST Special Publication 800 – 81(r1)
  - Deals with DNS Security, not just DNSSEC
  - NIST developed conformance tool to aid in auditing

- **Pilot / Operational Deployment in .gov**
  - ***Government as early adopter**.*
  - Work with GSA, NTIA, OMB to establish operational procedure for DNSSEC in the gov domain.
  - Operate pilot deployment: Secure Naming Infrastructure Pilot (SNIP)
  - Conducted .gov operator's workshops and training.



NIST Special Publication 800-xx

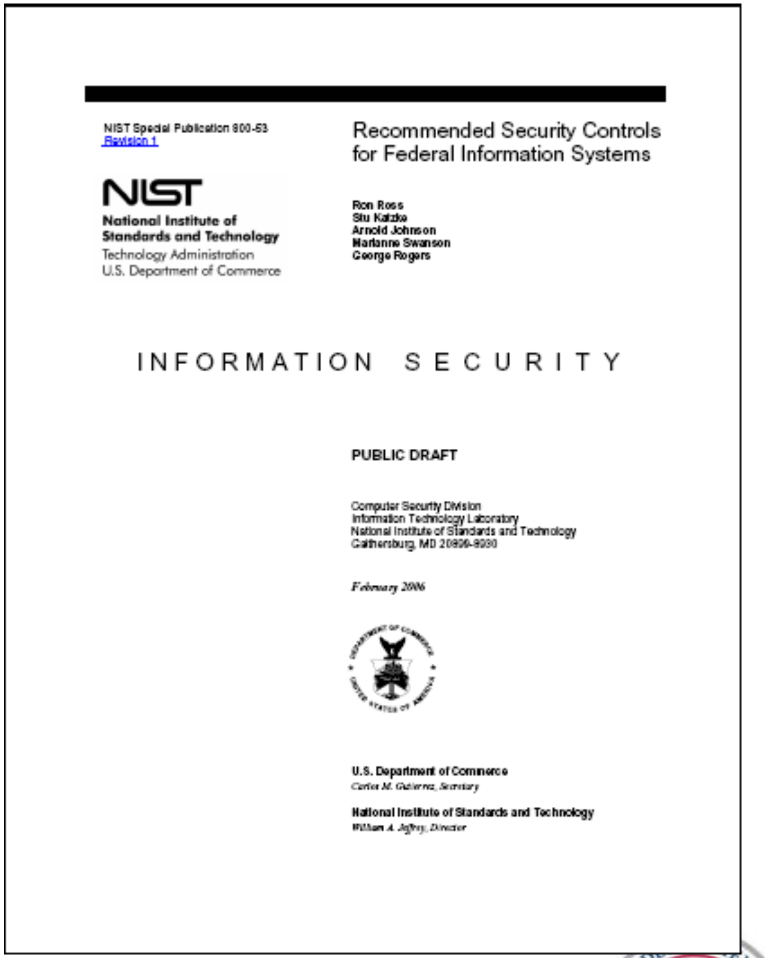
NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

COMPUTER SECURITY

Secure Domain Name System (DNS) Deployment Guide

DNSSEC and FISMA

- **Putting the FISMA Puzzle Together.**
- **FIPS-200** *Minimum Security Requirements for Federal Information Systems*
  - Points to NIST 800-53 *Recommended Security Controls for Federal Information Systems* for technical controls to meet these requirements.
- **NIST-800-53-r3**
  - Defines DNS security controls
  - Cites NIST 800-81 used as reference.
- **Promulgation – closing the loop.**
  - Final FIPS-200 published March 2006.
    - Effective immediately, 1 year for compliance according to FISMA
- **OMB memo M-08-23**
  - In line with FISMA deadlines
  - Special deadlines for .gov zone and all other Federal agencies



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 SP800-53r2

- SC-20 Secure Name/Address Resolution Service (Authoritative Source)
  - Will be pushed down to Low/Moderate/High in revision 3
  - DNSSEC signing of zone data
- SC-21 Secure Name/Address Revolution Service (Recursive or Caching Resolver)
  - For High category only
  - Recursive servers must be able to validate DNSSEC signed responses.
- SC-22 Architecture and Provisioning for Name/Address Resolution Service
  - Non-DNSSEC control
  - addresses other best security practices for DNS deployment and operation

Other NIST Resources

- Secure Naming Infrastructure Pilot (SNIP)
  - pilot domain acts as a distributed test lab
  - Completely voluntary
  - Organizations operate delegations (<zone>.dnsops.gov) to practice DNSSEC operations
    - Integrate DNSSEC into current operations
  - SNIP integrated into .gov operations
    - i.e. dnsops.gov has secure delegation from .gov
  - Also has vendor (non-gov) component dnsops.biz
    - http://www.dnsops.biz/vendors gives details on each

SNIP Impact

- **Stepping stone for operational use**
  - USG DNS operators get experience running delegation under dnsops.gov before deploying in own agency
- **Tool testing**
  - Tech transfer / training on existing tool suites (NIST, SPARTA, Shinkuro, ISC, et al).
- **Platform Testing**
  - Multi-vendor environment
    - Servers - ISC/BIND, NSD, Secure64 and more surprises
    - Resolvers – Linux, BSD, Microsoft, OS X
    - Applications – TBD.
- **Procedure Testing**
  - Refinement of procedure/policy guidance and reporting requirements

Lessons Learned from Early Deployments

- Deployment is really a content management exercise, not just a security exercise
  - FISMA, other drivers lead to centralization of many network operations
  - How is the data handled will help how best to deploy
- Signing is easy, key management is hard
  - Keys stored on machines, smart cards, hardware security modules (HSM)
  - key rollover/resigning done via homebrewed perl scripts to robust, fully functional COTS products
- Communication more important than strong crypto
  - Knowing who to contact (parent zone and subzones) important.
  - can be simple as email or web forms to complex M of N key generation ceremony

More Lessons Learned

- Upgrade vs. new purchases
  - Majority of agencies may not need investment in new equipment – upgrades may be enough, but it depends on current plans
    - May choose to for other reasons, but DNSSEC may not be the driver
- Invest the same importance in the keys as you do the data
  - There is such a thing as overkill
  - Consider information leakage as well
- Do not need to wait on anybody to deploy first
  - Majority of work is internal operations, interface to parent zone will be in a standard form
  - Practice makes perfect - SNIP

Resources

- Secure Name Infrastructure Pilot (SNIP)
  - http://www.dnsops.gov/
- NIST Publications Webpage
  - http://www.csrc.nist.gov/
- DNSSEC Deployment Initiative
  - http://www.dnssec-deployment.org/
- DNSSEC.net Resource page
  - http://www.dnssec.net/