NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Cyber and Network Security Program

DNS Security Extensions (DNSSEC) Briefing

Created by the DNSSEC-Deployment Initiative

Modified and Presented by Scott Rose, NIST

scottr@nist.gov

January , 2009

To put recent Internet vulnerabilities in context…

- Central role of DNS
  - the Internet's address system
- Why DNS is at risk
- DNSSEC: The Security Extensions
- Deployment Progress and Lessons Learned
- DNSSEC and FISMA
- Issues

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
- Used by anyone using Internet services:
  - Web browsing
  - Email
  - Voice Over Internet Protocol (VOIP) telecommunications

About DNS

- Maps name to IP address, other maps
  - For example, www.nist.gov = 129.6.13.23
- When users type URL, starts a series of DNS queries
- Each requires replies from the authoritative server to direct request accurately
- 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

NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

Why DNS Is At Risk: Threats and Attacks

- Attacks via and against DNS infrastructure are increasing
- Financial/large enterprises see major increases in online attacks for fraudulent purposes:
  - Hijacking – virtual theft of domain names
  - Phishing – look-alike fraudulent emails, sites
  - Pharming – phishing + DNS attacks
- Tools available: no learning curve required

Why DNS Is At Risk: Threats and Attacks

- DNS on ‘top 20’ list of Internet security attack targets by SANS Institute
- PC World Canada puts it in top 10 biggest security risks facing business
  - Notes that more than a million DNS servers running old or misconfigured DNS software, exacerbating the problem for more than 75 percent of all servers worldwide

Why DNS Is At Risk: Threats and Attacks

- Attacks becoming costly and difficult to remedy
- Consumer confidence decreasing
- DNS seen as critical weakness in National Strategy to Secure Cyberspace (2003)
- According to March 2008 survey by International Chamber of Commerce, over 1,000 economic experts from 90 countries said that a one-day Internet blackout would mean "major losses and costly damage…huge and lasting effects."

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
- Detects and addresses attacks independent of software holes
  - DNS software part of problem

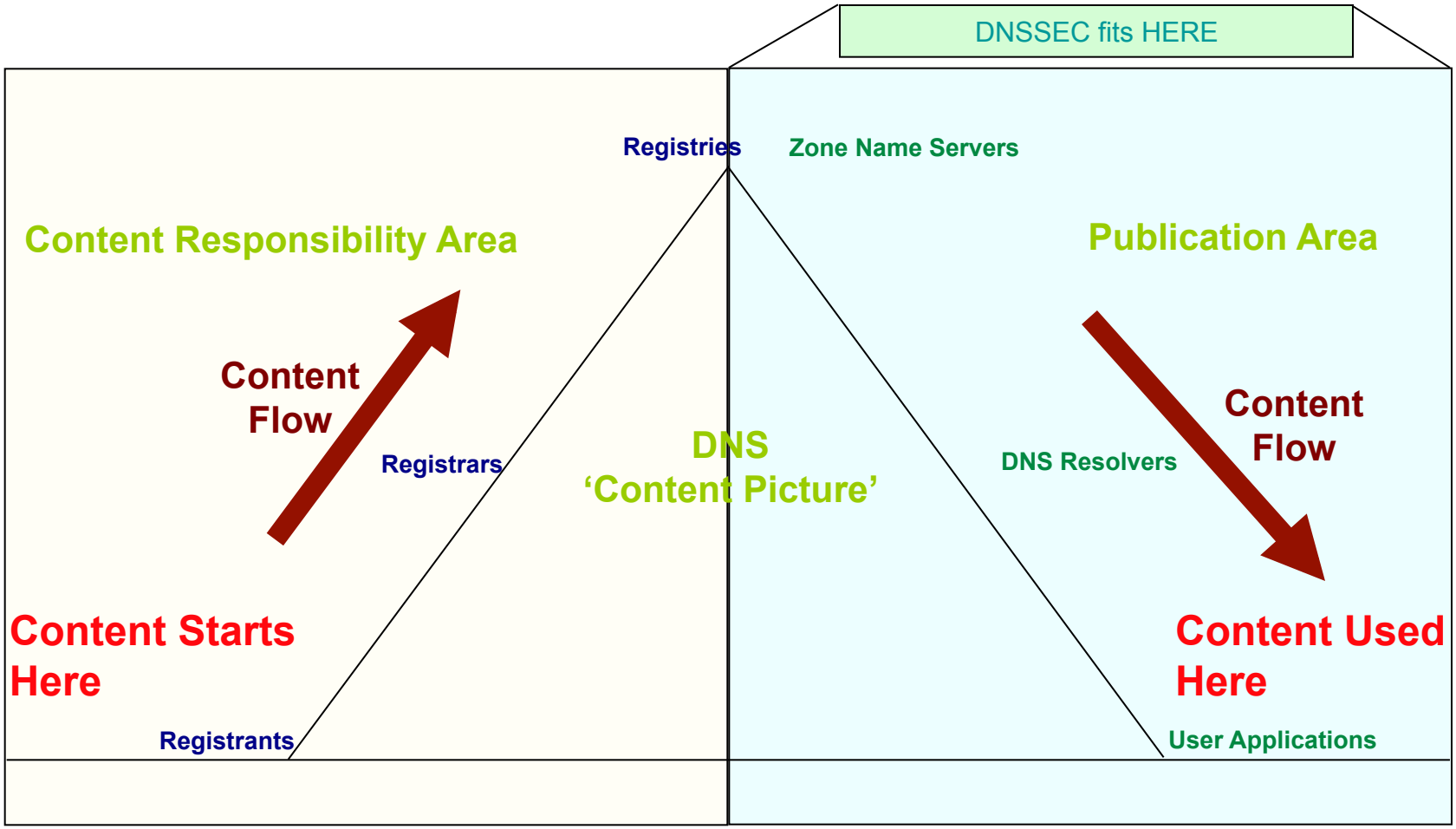
What DNSSEC Provides

- 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

Where Does DNSSEC Fit?

- 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

Where Does DNSSEC Fit?



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, or allow opt-ins

DNSSEC Deployment

- US Department of Homeland Security Science & Technology Directorate programs
  - DNSSEC
  - Secure Protocols for the Routing Infrastructure
  - Protected Repository for the Defense of Infrastructure against Cyber Threats
- DHS cannot secure Internet by itself
  - Taking leadership role, facilitating public-private partnerships

Deployment Progress

- Early adopters include:
  - Country-code top-level domains: Brazil, Bulgaria, Puerto Rico and Sweden
  - Public Interest Registry for .org top-level domain
  - Verisign pilot testbed for .com and .net
  - .arpa signed
  - nist.gov first US agency to sign as part of normal DNS operations
- Deployment initiative working with Microsoft, Mozilla, OLPC, OpenDNS, others to promote DNSSEC awareness in software or other projects

Lessons Learned from Early Deployments

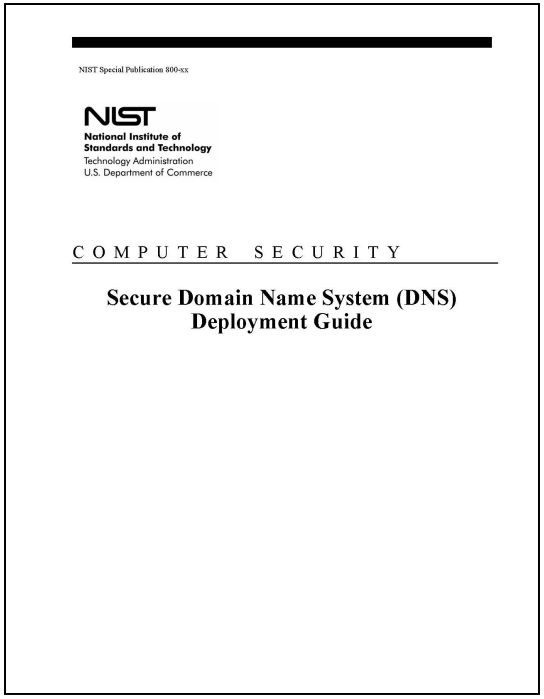
- Deployment is really a content management exercise, not just a security exercise
  - FISMA, other drivers lead to centralization of many network operations
  - How is the data handled will help how best to deploy
- Signing is easy, key management is hard
  - Keys stored on machines, smart cards, hardware 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

DNSSEC Guidance

- **Secure DNS Guidance Documents**
  - NIST Special Publication 800 - 81
  - 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

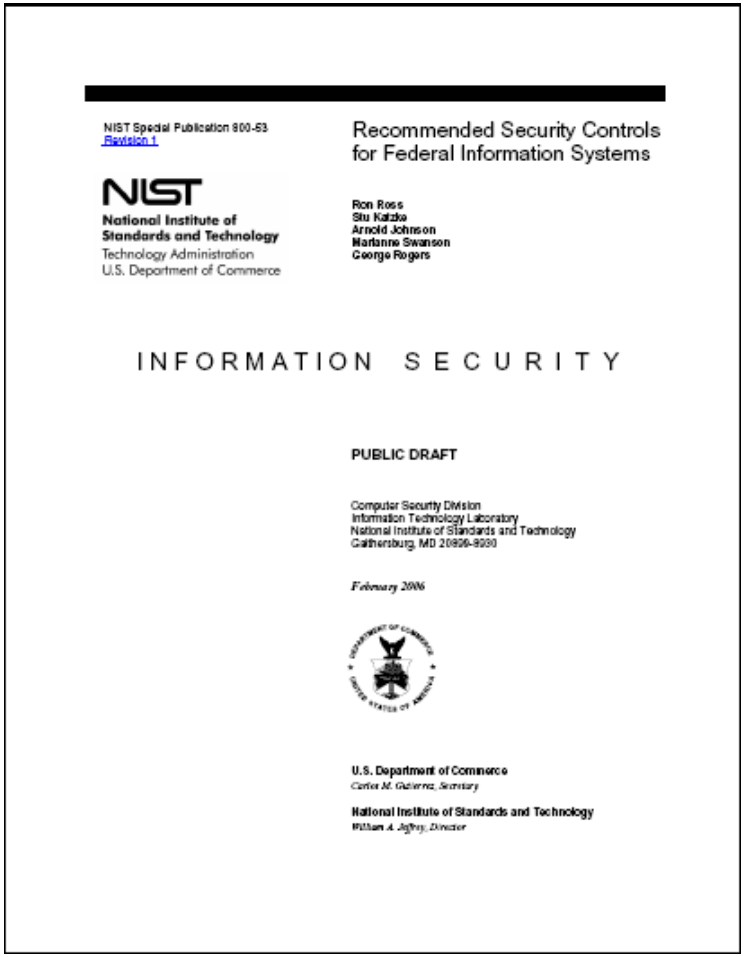
NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

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-880-53 *Recommended Security Controls for Federal Information Systems* for technical controls to meet these requirements.
- **NIST-800-53-r2**
  - 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
- **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-8 Transmission Integrity
  - 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 Moderate and High
  - Will be pushed down to Low/Moderate/High in revision 3
  - DNSSEC signing of zone data
  - Reference: NIST SP800-81

DNS Related Controls in SP800-53r2

- SC-21 Secure Name/Address Revolution Service (Recursive or Caching Resolver)
  - For High category only
  - Not expected to change in revision 3
  - 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
  - Non-DNSSEC control
  - addresses other best security practices for DNS deployment and operation
  - Should be Moderate/High in revision 3

NIST SP 800-53A

- Gives guidance on how to check if controls are met
  - Goes through each control and gives assessment objectives and checks based on security classification (Low, Moderate or High)
  - Assessment recommendations given in Examine/Test language
    - Examine: policy document, plans, architecture, etc.
    - Test: server configuration, messages, etc.

NIST SP800-57 Recommendations for Key Management

- 3 Part guide on Federal key management practices.
  - Part 1 General: Defines scope, gives overview of process, crypto algorithms and procedures and terms used in the document series.
  - Part 2 Best Practices for Key Management Organization: Identifies requirements, and policies for IT organizations.
  - Part 3 Application Specific Key Management Guidance: Gives specific guidelines for procurement and configuration of software to support given applications

DNSSEC in SP800-57 Part 3

- Procurement
  - What crypto algorithms, hash algorithms, and key sizes a software product must and should support
- System Installers
  - Configuration recommendations.
- Server Administrators
  - restating checklist items in NIST SP800-81
  - Except in cryptographic related parameters
- Cache/Recursive Server Administrators

Resources

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