

Domain Name System Security (DNSSEC)

**CA CISO Lecture Series
Sacramento, CA
December 15, 2009**



***Douglas Maughan, Ph.D.
Program Manager, CCI
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170***



Agenda

- **What is the Domain Name System (DNS)?**
- What is DNS Security (DNSSEC)?
- What is the U.S. Government doing with DNSSEC?
 - ◆ Who's involved? DHS, OMB, GSA, NIST
 - ◆ How might that impact State and Local governments?
 - ◆ What help is available?
- What vendors have DNSSEC capable products?
 - ◆ What questions should I ask the vendors?
- Summary / Conclusions



The Domain Name System (DNS) is ...

- What Internet users use to reference anything by name on the Internet
- The mechanism by which applications get translations of names to IP addresses and vice versa
- A globally distributed, loosely coherent, scalable, reliable, dynamic database
- Comprised of two primary types of components
 - ◆ The information itself, sometimes called the “name space” or “DNS Content”
 - ◆ The “moving parts” that provide the means for users to get information - can be further divided to:
 - Servers that provide answers to the DNS questions
 - Resolvers (clients) which ask questions about DNS information



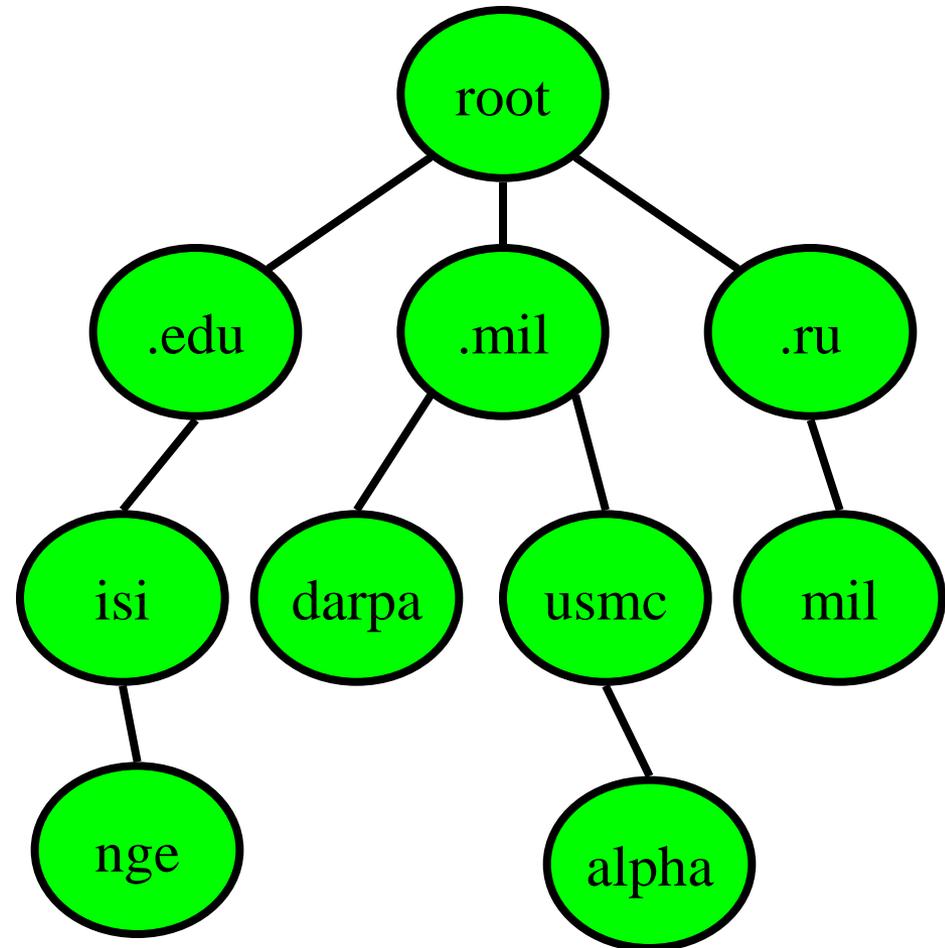
The Domain Name System

- DNS database maps:

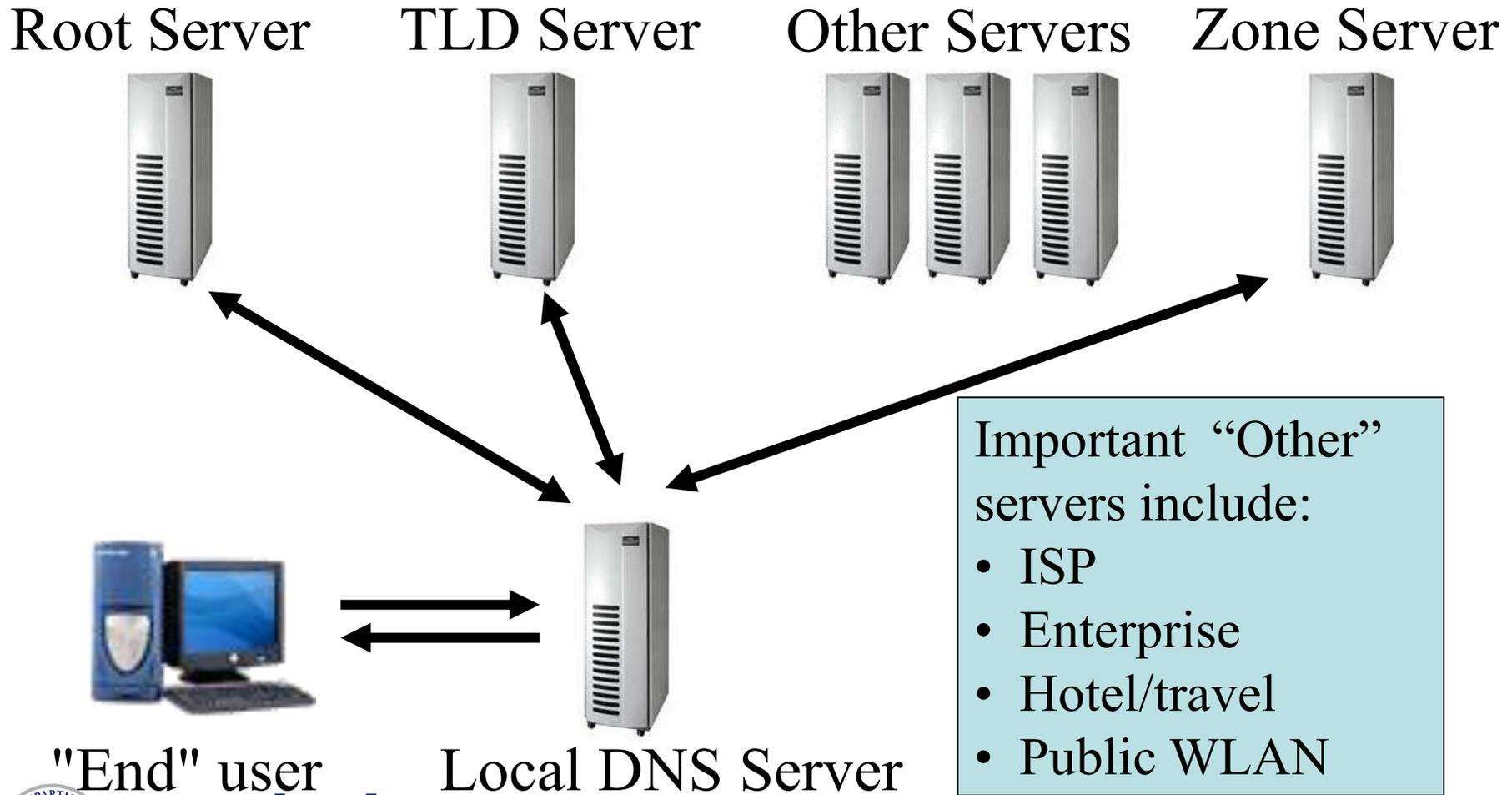
- ◆ Name to IP address
www.dhs.gov = **206.18.104.198**
- ◆ And many other mappings
(mail servers, IPv6, reverse...)

- Data organized as tree structure:

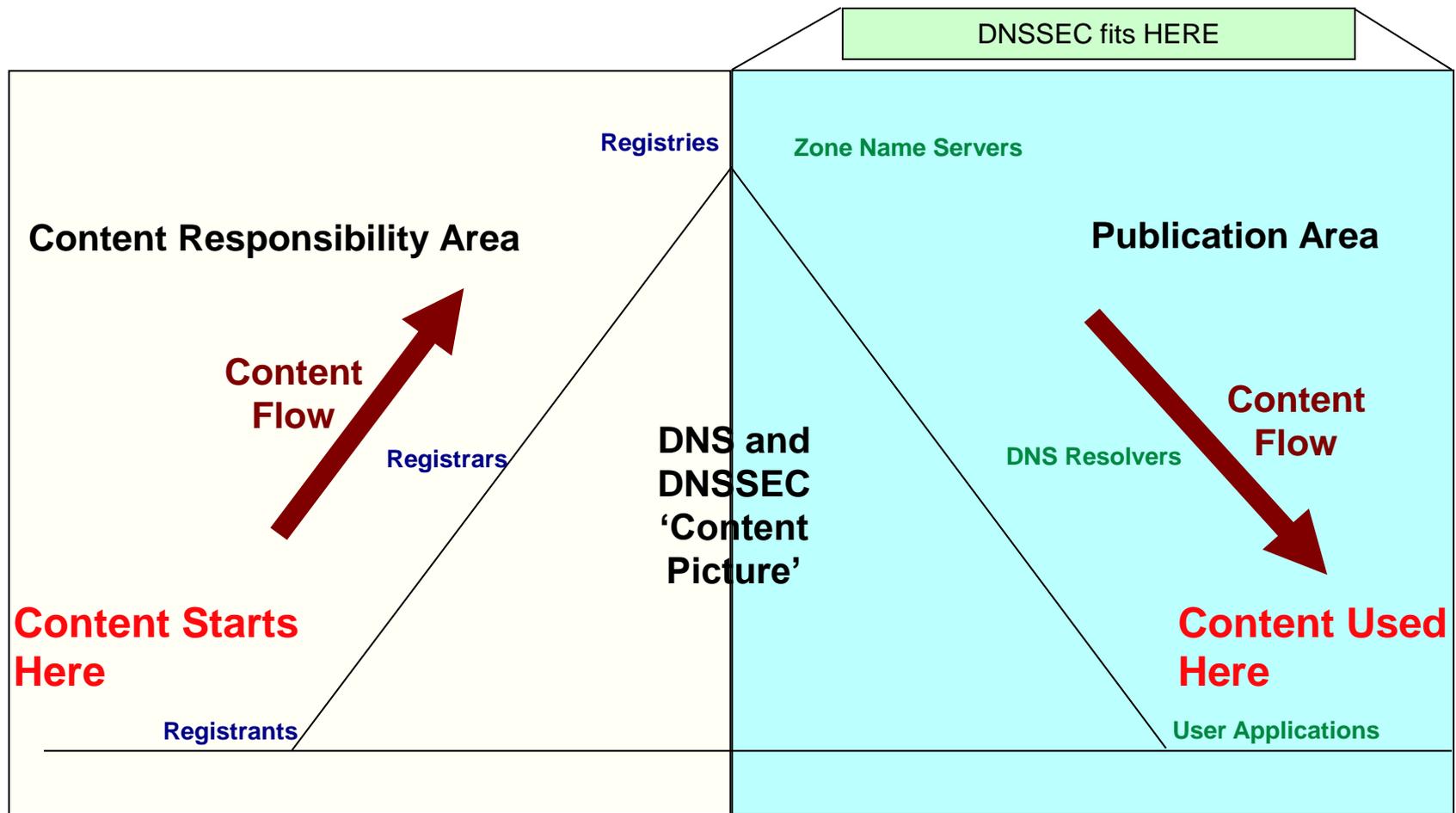
- ◆ Each zone is authoritative for its own data
- ◆ Minimal coordination between zone operators



DNS Name Resolution



What and Who are the DNS (and DNSSEC) Players and Pieces?



Agenda

- What is the Domain Name System (DNS)?
- What is DNS Security (DNSSEC)?
- What is the U.S. Government doing with DNSSEC?
 - ◆ Who's involved? DHS, OMB, GSA, NIST
 - ◆ How might that impact State and Local governments?
 - ◆ What help is available?
- What vendors have DNSSEC capable products?
 - ◆ What questions should I ask the vendors?
- Summary / Conclusions



Why is the DNS so Vulnerable?

- Designed in 1980s when the trust model and the threat model were very different from today
 - ◆ Attack the trust model and you can change the way information is found and exchanged on the Internet
- Optimized for fast query/response times
 - ◆ Not optimized for authenticity or integrity
 - ◆ Trust is implied - legitimate queries and legitimate replies are expected
- DNS threats identified in early 1990s
- Attacks via DNS and against the DNS are increasing
 - ◆ August 2008 – Kaminsky bug is a prime example
 - ◆ Attacks are becoming costly and difficult to remedy



Cache Poisoning (Kaminsky) Attack.

- Technically nothing new
 - ◆ Vulnerability identified in '95 at least.
- What opened eyes:
 - ◆ ...was the **scope of vulnerability** – millions of DNS servers.
 - ◆ ... was the **ease of executing the attack**.
 - ◆ ... was the novel ways in which cache poisoning could be used as a tool to **undermine other critical network services and trust models**.
- What people are learning:
 - ◆ Is that there is no simple quick fix.
 - ◆ “The patch” – while important – only moved the vulnerability from trivial to exploit to easy to exploit
 - ◆ The Kaminsky attacks will continue – software available, patched systems proven still vulnerable.
 - ◆ **The Kaminsky attack is just the latest instance to exploit a systemic DNS vulnerability. There are and will be more..**

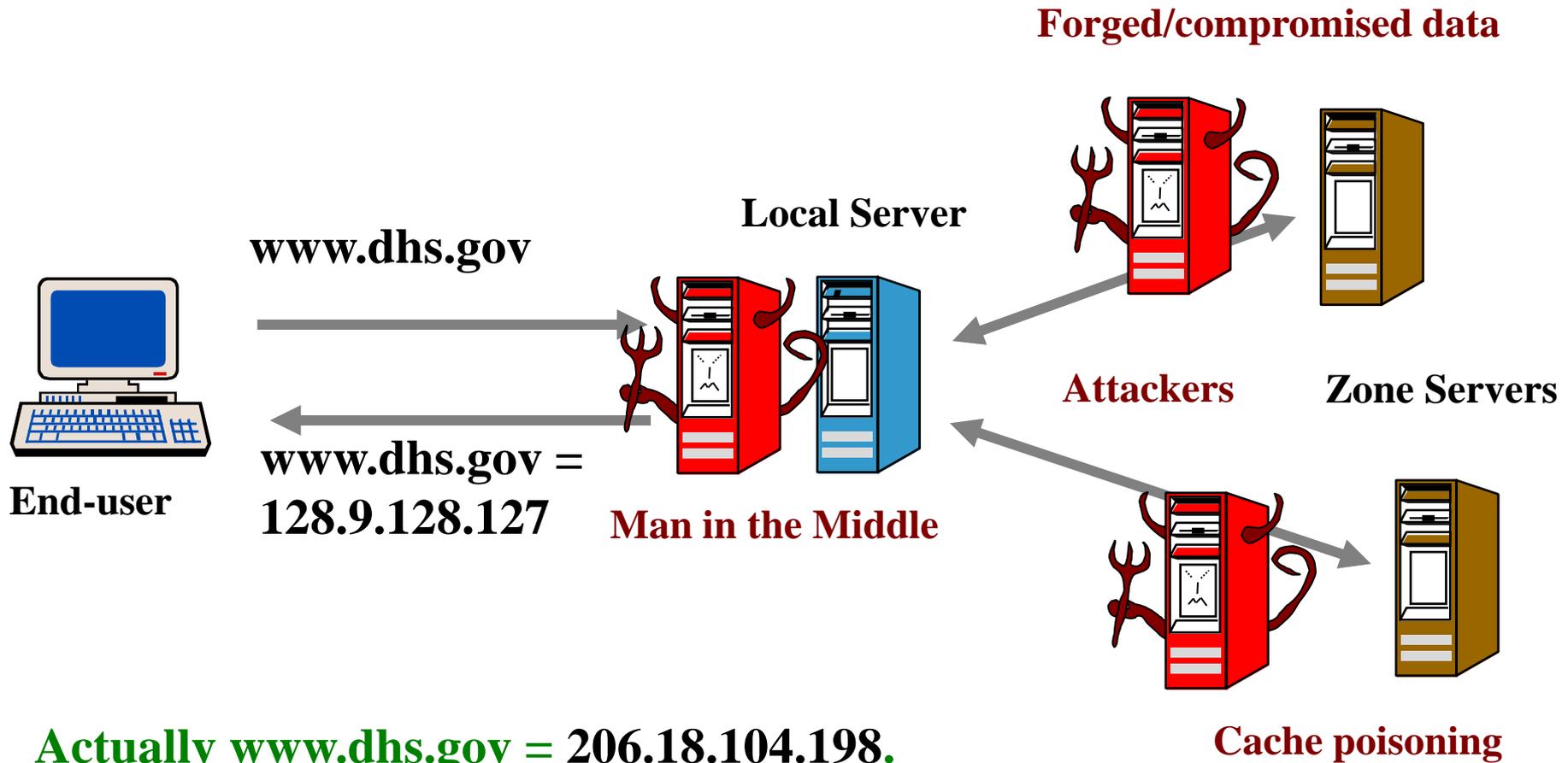


What Does DNSSEC Do?

- Provides an approach so DNS users can:
 - ◆ Validate that data they receive came from the correct originator → Source Authenticity
 - ◆ Validate that data they receive is the data the originator put into the DNS → Data Integrity
- This approach integrates with existing server infrastructure and user clients
- Maximized benefit when application software can determine if DNS data was received with authenticity and integrity
- Not provided by DNSSEC: message encryption, security for denial-of-service attacks



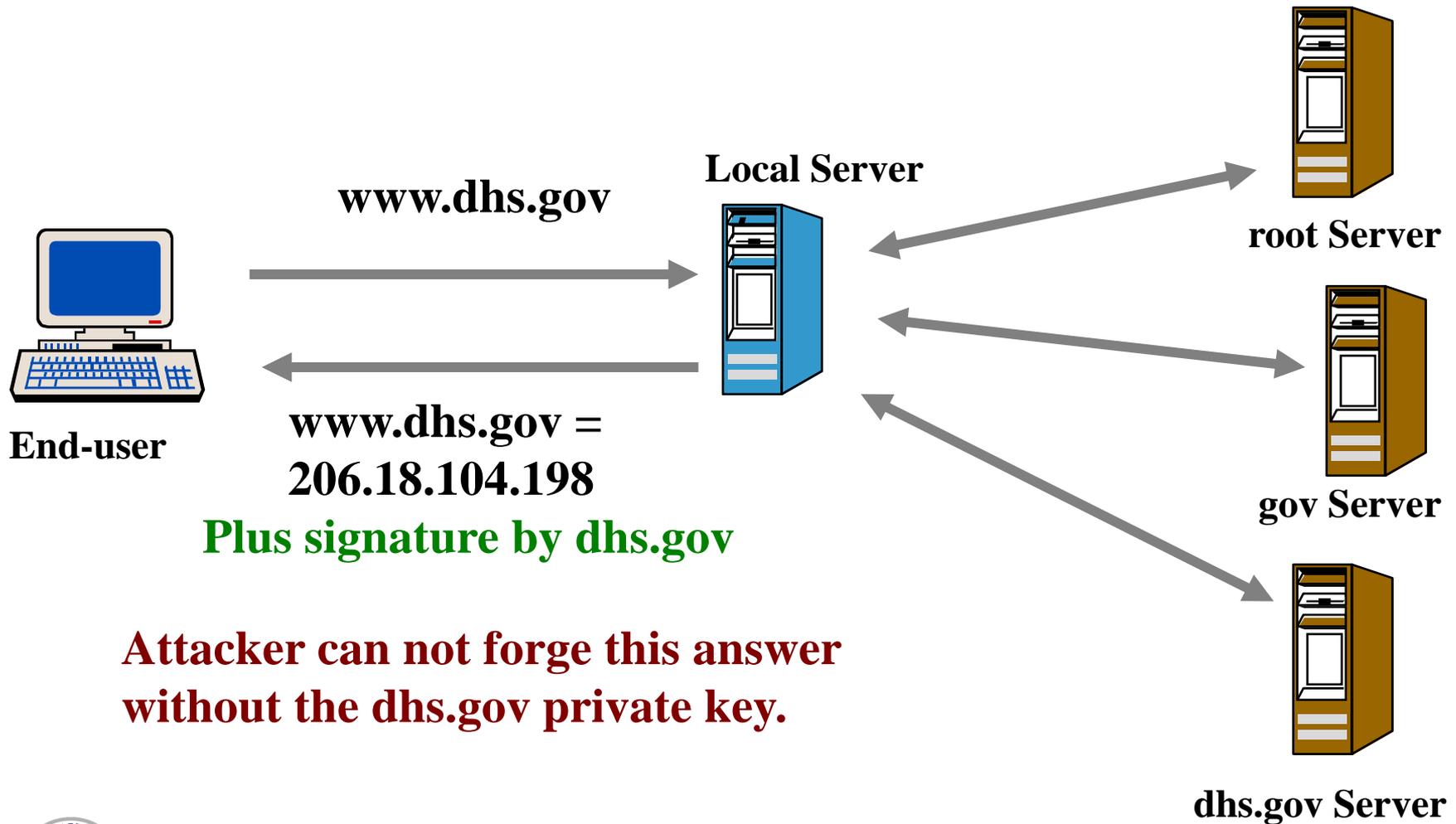
DNS Attacks – Graphical View



**Actually www.dhs.gov = 206.18.104.198.
But how do you determine this?**



Secure DNS Query and Response



**Attacker can not forge this answer
without the dhs.gov private key.**



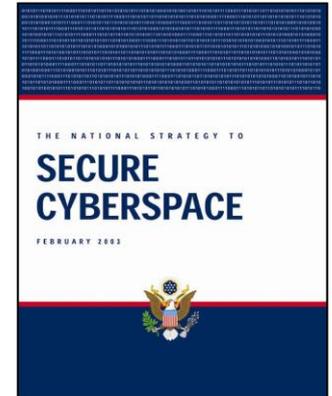
Agenda

- What is the Domain Name System (DNS)?
- What is DNS Security (DNSSEC)?
- What is the U.S. Government doing with DNSSEC?
 - ◆ Who's involved? DHS, OMB, GSA, NIST
 - ◆ How might that impact State and Local governments?
 - ◆ What help is available?
- What vendors have DNSSEC capable products?
 - ◆ What questions should I ask the vendors?
- Summary / Conclusions



National Strategy to Secure Cyberspace

- The National Strategy to Secure Cyberspace (2003) recognized the DNS as a critical weakness
 - ◆ NSSC called for the Department of Homeland Security to coordinate public-private partnerships to encourage the adoption of improved security protocols, such as DNS
 - ◆ **The security and continued functioning of the Internet will be greatly influenced by the success or failure of implementing more secure and more robust BGP and DNS.** The Nation has a vital interest in ensuring that this work proceeds. **The government should play a role when private efforts break down due to a need for coordination or a lack of proper incentives.**



Homeland
Security

DNSSEC Initiative Performers

- Shinkuro, Washington, DC

- ◆ Roadmap Development and Execution
 - International partner participation
- ◆ Support Tool Development



- Sparta, Columbia, MD

- ◆ Software Development – Servers, resolvers, applications
- ◆ Internet Standards activities



- NIST, Gaithersburg, MD

- ◆ Measurement and Evaluation Tools
- ◆ Government and Standards activities
 - Connections with GSA, FISMA, and OMB



**Homeland
Security**

DNSSEC Initiative Activities

- Roadmap published in February 2005; Revised March 2007
 - ◆ <http://www.dnssec-deployment.org/roadmap.php>
- Multiple workshops held world-wide
- Involvement with numerous deployment pilots
- DNSSEC testbed developed by NIST
 - ◆ <http://www.dnsops.gov/>
- Formal publicity and awareness plan including newsletter
 - ◆ <http://www.dnssec-deployment.org/news/dnssecthismonth>
- Working with Civilian government (.gov) to develop policy and technical guidance for secure DNS operations and beginning deployment activities at all levels.
- Working with Microsoft, Mozilla, OpenDNS and others to promote DNSSEC capability and awareness in their software or projects



DNSSEC Roadmap

- <http://www.dnssec-deployment.org>
- Identifies the following activities:
 - ◆ Remaining R&D Issues (Lead: Shinkuro)
 - ◆ Software Development (Lead: Sparta)
 - Server
 - Resolver
 - Applications
 - ◆ Operational Considerations (Lead: Shinkuro)
 - Root
 - Registries
 - Registrants
 - ◆ Measurement and Evaluation (Lead: NIST)
 - ◆ Outreach and Training (Lead: Shinkuro)



DNSSEC Current State

- RFC 4033
 - ◆ DNS Security Introduction and Requirements
- RFC 4034
 - ◆ Resource Records for the DNS Security Extensions
- RFC 4035
 - ◆ Protocol Modifications for the DNS Security Extensions
- RFC 5011
 - ◆ DNS Key Rollover
- RFC 5155
 - ◆ DNSSEC Hashed Authenticated Denial of Existence
- <http://www.dnssec.net/rfc> for the entire collection



DNSSEC Tools

- <http://www.dnssec-tools.org>
- Identifies the following available open-source tools:
 - ◆ Authoritative Zones
 - ◆ Authoritative Servers
 - ◆ Recursive Servers
 - ◆ Applications
 - ◆ Application Developers



Incremental Deployment

- Registries
 - ◆ Work through various readiness levels
 - Initial study -> Initial design -> Pilot -> Pre-deployment -> Operation
- Registrars
 - ◆ Migrate to an Extensible Provisioning Protocol (EPP)-based system
 - ◆ Build extensions for existing non-EPP system
- ISPs
 - ◆ Validation as a preferred service for some customers. Requires managing customized set of Trust Anchors for sets of customers
 - ◆ Detect key rollover events for known islands of trust
- Enterprise
 - ◆ Internal deployment as part of corporate system integrity and protection
 - ◆ Trading partners
 - ◆ Distinguish between safe and questionable sites



Leveraging Existing Efforts

- ccTLDs with operational DNSSEC Services
 - ◆ Sweden: <http://www.iis.se/products/sednssec2>
 - ◆ Bulgaria: <https://www.register.bg/>
 - ◆ Brazil: <https://www.registro.br>
 - ◆ Puerto Rico: <http://www.dnssec.nic.pr/>
 - ◆ The Czech Republic: <http://www.dnssec.cz/>
- RIPE-NCC
 - ◆ Reverse zones that it manages and e164.arpa zone (ENUM)
 - ◆ <https://www.ripe.net/rs/>
- DNSSEC initiatives in .UK and .DE
 - ◆ Strong advocates of DNSSEC, implementation in progress
 - ◆ <http://www.denic.de/en/domains/dnssec/index.html> and <http://www.nominet.org.uk/tech/dnssectest/>
- JPRS
 - ◆ Working on integrating DNSSEC signing into existing workflow to maintain short update assurances - <http://losangeles2007.icann.org/node/77>



Leveraging Existing Efforts (cont)

- .ORG testbed
 - ◆ PIR has maintained the .ORG testbed to enable its registrars to test DNSSEC-capable systems
 - ◆ <http://www.pir.org/RegistrarResources/DNSSecurityTestbed.aspx>
- SNIP testbed for .GOV
 - ◆ Provide “distributed training ground” for .gov operators deploying DNSSEC
 - ◆ <http://www.dnsops.gov>
- IANA
 - ◆ Testbed for signing zones that IANA controls
 - ◆ Also has a prototype for a signed copy of the Root zone
 - ◆ <https://ns.iana.org/dnssec/status.html>



NIST Effort - SNIP

- Secure Naming Infrastructure Pilot (SNIP)
- Aiding deployment by:
 - ◆ Providing a connected training ground
 - ◆ Educational resources/guides
 - ◆ Modeling infrastructures
 - ◆ Testbed for systems
- Relying on user participation
 - ◆ Aid in deployment, not a proof-of-concept experiment



USG Road to Deployment

- Not a Chicken and Egg Problem!
 - ◆ Clear answer is to establish signed infrastructure first
 - ◆ ... then deploy validators/applications to use it.
- Phased Development & Deployment Plan
 - ◆ Phase 1 2000-2008
 - Technology Development and Testing
 - Deployment Guidance
 - ◆ Phase 2 2008-2010
 - Sign the USG DNS Infrastructure (.gov)
 - ◆ Phase 3 2010+
 - Deploy validation tools to leverage signed infrastructure.
 - Deploy DNSSEC-aware applications.



Recommendations, Requirements and Policies

- Embodied in evolving FISMA Requirements:
 - ◆ FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems
 - ◆ (FISMA) **Recommended Security Controls for Federal Information Systems (NIST SP 800-53)**
 - ◆ (FISMA) Guide for Assessing the Security Controls in Federal Information Systems (NIST SP 800-53A)
 - ◆ **Secure Domain Name System (DNS) Deployment Guide (NIST SP 800-81).**
 - ◆ Recommendation for Key Management (NIST SP 800-57).
- Embodied in specific policies:
 - ◆ **Securing the Federal Government's Domain Name System Infrastructure (OMB M-08-23)**



OMB memo on DNSSEC



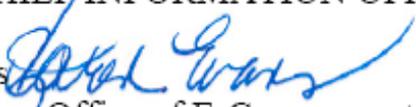
EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

<http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf>

August 22, 2008

M-08-23

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans 
Administrator, Office of E-Government and Information Technology

SUBJECT: Securing the Federal Government's Domain Name System Infrastructure
(Submission of Draft Agency Plans Due by September 5, 2008)

The efficient and effective use of our networks is important to promote a more citizen centered and results oriented government. The Government's reliance on the Internet to disseminate and provide access to information has increased significantly over the years, as have the risks associated with potential unauthorized use, compromise, and loss of the .gov domain space.

Almost every instance of network communication begins with a request to the Domain Name System (DNS) to resolve a human readable name for a network resource (e.g., www.usa.gov) into the technical information (e.g., Internet Protocol address) necessary to actually access the remote resource. This memorandum describes existing and new policies for deploying Domain Name System Security (DNSSEC) to all Federal information systems by December 2009

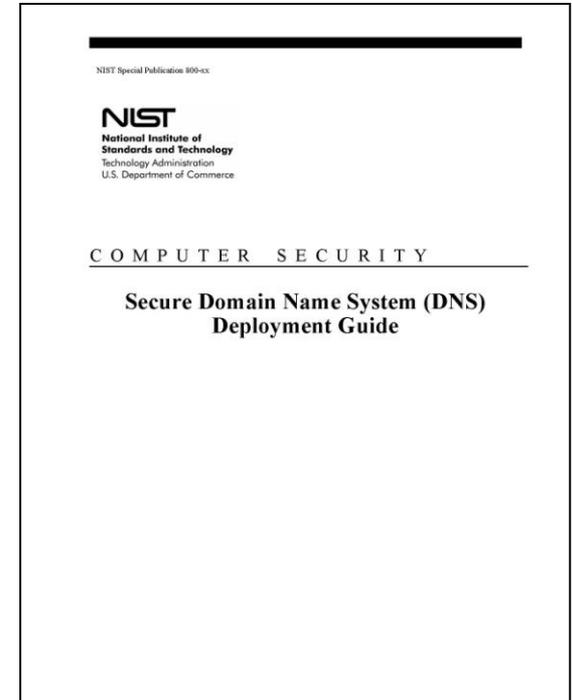
OMB DNSSEC Memo

- Discussions began back in 2006 with OMB/OSTP
- Specific Purposes:
 - ◆ Introduction to DNSSEC
 - ◆ Reminder of existing security controls
 - ◆ Announcement of plans to sign .gov domain
 - ◆ Instructions for each agency to develop plans for the deployment of DNSSEC to all applicable systems
 - ◆ Identifies other sources of information
 - ◆ Discusses training available (from DNSSEC team)



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.
- **NIST SP800-81r1** – to be released any day
 - ◆ 1024 bit RSA/SHA-1 (or RSA/SHA-256) ZSK's still allowed until 2015
 - ◆ Expected that Elliptic Curve will be specified and implemented by then.
 - ◆ Note that the Root will begin signing using RSA/SHA-256.



What is Required When?

- **Phase 2 – Sign the USG Infrastructure**
 - ◆ FISMA Dec 2006 Revision
 - Required HIGH & MODERATE impact systems to sign and HIGH *to be able to* validate zones.
 - ◆ Aug 2008 OMB-08-23
 - Requires .gov TLD to be signed by early 2009.
 - External facing agency .gov zones to be signed by Dec 2009.
 - Agencies to comply with 2009 FISMA DNSSEC requirements.
 - ◆ FISMA May 2009 Revision
 - All (HIGH, MODERATE, LOW) systems must sign DNS by May 2010.
- **Phase 3 – Validation / Application Infrastructure**
 - ◆ Target FISMA 2010 Revision.



GSA - .GOV Program Overview

- GSA became the managing partner Agency in 1997
 - ◆ Governing document is the Code of Federal Regulations Final Rule 41 CFR Part §102-173 (March 28, 2003).
 - ◆ Federal, state and local government organizations, and Native Sovereign Nations (NSNs) may register a .GOV top level domain (TLD) name on the Internet at www.dotgov.gov.
- GSA charges an annual fee for a .GOV domain name.
 - ◆ GSA's .GOV program is the only source in the world for obtaining a .GOV domain name.
 - ◆ Extremely high visibility program
 - ◆ 24x7 helpdesk emergency support
- Total of 4,705 registered .GOV domain names (February 25, 2009).
 - ◆ Active Federal 1,748
 - ◆ Active State/Local 2,438
 - ◆ Active NSN 107
 - ◆ Awaiting info to activate 412



.GOV DNSSEC Deployment – Support to Agencies

- DNSSEC Registration Support
 - ◆ Self registration through www.dotgov.gov
 - ◆ Automated monitoring
- Policy Support and Lessons Learned
 - ◆ DNSSEC FAQ and policies available on www.dotgov.gov
- Open testing environment for Agencies ready to implement DNSSEC
 - ◆ Seamless integration with NIST's SNIP test environment to allow Agencies/Departments/States/Locals a safe place to test and work through DNSSEC issues
- Live Help Desk Support
 - ◆ 877-734-4688
registrar@dotgov.gov



Government Domain Registration and Services

[MyDOTGOV](#)

SEARCH

HOME

REGISTER

WHOIS

MY ACCOUNT

POLICY

NEWS

DNSSEC - New!

Logged in as **gsg1** | [Log Out](#) | [Site Map](#) | [FAQ](#) | [Customer Support](#)

DNSSEC UPDATE

The DotGov program has completed DNSSEC testing and is now fully operational. For DNSSEC validation, the latest gov public key is available ['here'](#) and should be used as the published trust anchor for .gov. Please visit the new DNSSEC tab at the top of this page for more information.

NOTICE: All unpaid .Gov domain names must be paid for via credit card ASAP or they will be subject to service interruption.

For a copy of the IRS Form W-9, please [Click Here](#)

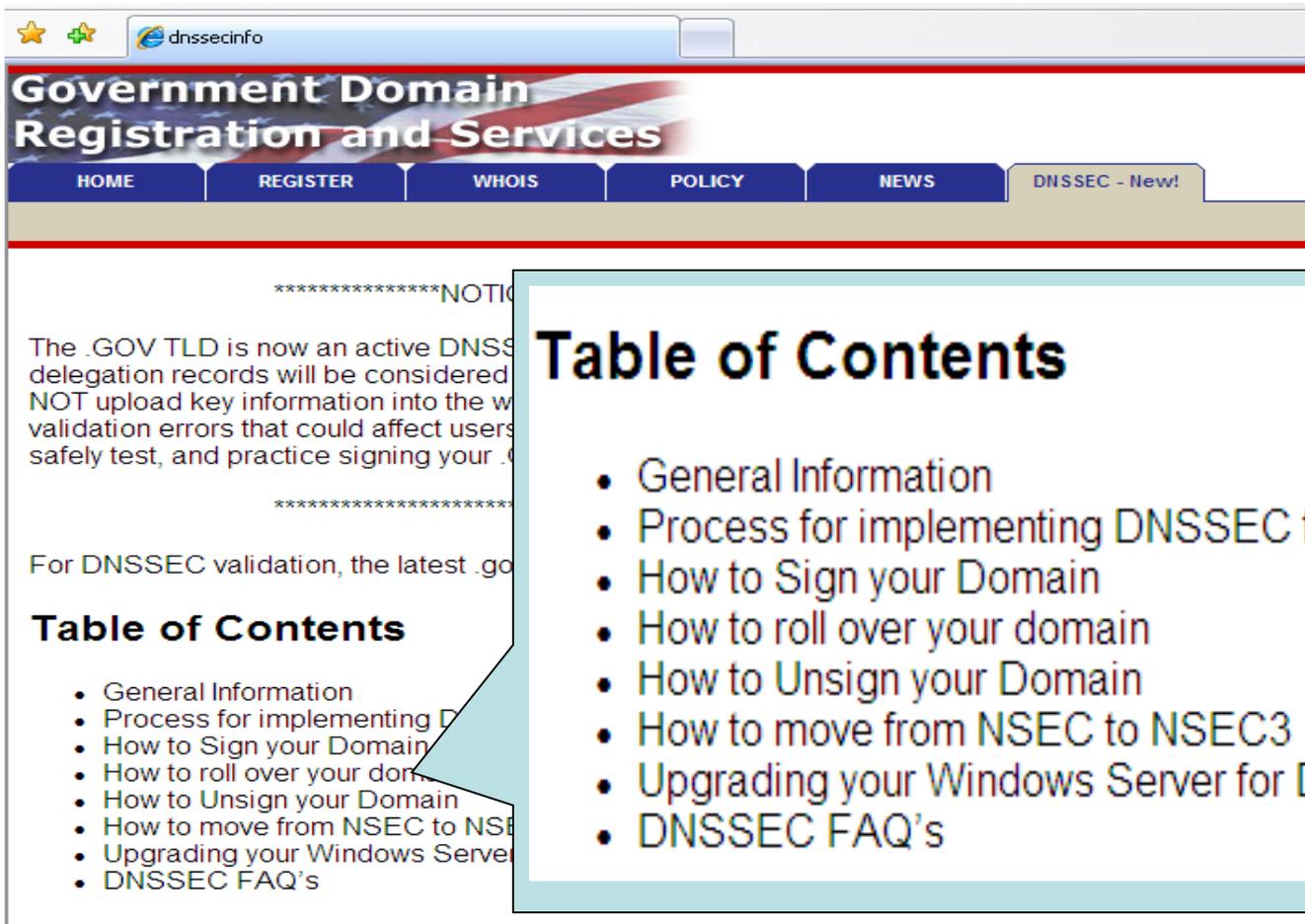
You have reached the General Services Administration (GSA) website for



security



.GOV – DNSSEC where to get info



The screenshot shows a web browser window with the address bar containing 'dnssecinfo'. The page title is 'Government Domain Registration and Services'. The navigation menu includes 'HOME', 'REGISTER', 'WHOIS', 'POLICY', 'NEWS', and 'DNSSEC - New!'. The main content area features a 'Table of Contents' callout box with the following items:

- General Information
- Process for implementing DNSSEC for your .GOV Domain
- How to Sign your Domain
- How to roll over your domain
- How to Unsign your Domain
- How to move from NSEC to NSEC3
- Upgrading your Windows Server for DNSSEC
- DNSSEC FAQ's



.GOV – DNSSEC FAQ's

[Home](#) » [DNSSEC FAQ](#)

[Domain Signing](#)

[KSK Management](#)

[ZSK Management](#)

[.gov Registrar Key Monitor](#)

Domain Signing

- [How do I sign a .gov domain?](#)
- [How do I unsign a .gov domain?](#)
- [When do I have to sign my .gov domains?](#)

[Top of Page](#)

KSK Management

- [What is the KSK and how is it used?](#)
- [How do I change from NSEC KSK keys to NEC3 KSK keys?](#)
- [Where do I find the .gov public KSK \(trust anchor\) and how do I use it?](#)
- [How do I publish my domain's public KSK?](#)

[Top of Page](#)

ZSK Management

- [What is the ZSK and why do I need it?](#)
- [How often should I roll my ZSK?](#)
- [Why do the .gov zone signing instructions have me create 2 ZSKs?](#)
- [Do I need to upload my domain's public ZSK to the .gov TLD?](#)



.GOV – DNSSEC Registration

[Click here for .gov TLD DNSSEC Features](#)

BASIC DNS Security (DNSSEC)

Upload DNSKEY file(keyset file): Sign one or more domain(s) and upload the public keyset file(s) to enable DNSSEC.

Tip: Multiple domains will be updated if *dnssec-signzone* KEYSET files are merged into a single file.

[CLICK HERE TO PRACTICE DNSSEC DOMAIN PROCEDURES BY USING THIS INTERFACE TO PUBLISH TO THE DNSSEC TESTBED \(SNIP\)](#)

[Signzone Instructions](#)

[DNSSEC FAQs](#)

Optional DNS Security (DNSSEC)

Select your DNSSEC Option: You may choose to allow dotgov.gov to generate, monitor, and automatically update DS Resource Records for none, some, or all of your domains.

- No, thanks. I will manually upload my keysets after I have pre-published my KSK (bi-annually).**
- Yes, but only for domains I select below. I will manually upload keysets for unchecked domains.**
- Yes. Monitor and automatically publish DS RRs for all my domains.**

| Domains | | | | | |
|---------|------------------------|-----------------|---|---|---|
| Pay | Domain Name | Expiration Date | Past Payments | Online Domain Tools | DNS Security (DNSSEC) |
| | FED.US | 9/15/2009 | 7/22/2005 Donna Samblanet Print Receipt | Run Report GSA does not endorse or warranty providers of online DNS tools. | DS Resource Records: Tips Not Enabled. To enable DNSSEC, upload a dsset file for this domain. |
| | | | 2/7/2006 Donna Samblanet Print Receipt | | DNSKEY (public Key): Tips Not Enabled. To enable DNSSEC features, upload a keyset file for this domain. |
| | | | 2/7/2006 Donna Samblanet | | |



Agenda

- What is the Domain Name System (DNS)?
- What is DNS Security (DNSSEC)?
- What is the U.S. Government doing with DNSSEC?
 - ◆ Who's involved? DHS, OMB, GSA, NIST
 - ◆ How might that impact State and Local governments?
 - ◆ What help is available?
- What vendors have DNSSEC capable products?
 - ◆ What questions should I ask the vendors?
- Summary / Conclusions



Questions to ask the Vendors

- GovSec 2009 - http://wordpress.test.dnssec-deployment.org/?page_id=62
- The Basics:
 - ◆ Does it do DNSSEC according to the most recent RFC's? (RFC 4033, 4034, and 4035)
 - ◆ Do your products have FIPS 140 certification?
 - ◆ Does it generate keys of the appropriate size? (2048 bit RSA/SHA-1)
 - ◆ Can the product be used to manage key material?
 - ◆ Can the product generate both NSEC and NSEC3 signed zones?
 - ◆ Can I sign/serve/manage multiple zones using this product?



Questions to ask the Vendors (cont'd)

- The Not-So-Basics:
 - ◆ Does it integrate with <your content management system>?
 - ◆ Does it work in your network infrastructure?
 - ◆ Does it work with MS Active Directory/Your DHCP server of Choice?
 - ◆ Can you use an HSM for key management with your product?
 - ◆ How do you update zone data using your product?
 - ◆ What about logging/debugging tools?



DNSSEC Product Vendors - 1

- AEP Networks

- ◆ Somerset, New Jersey

- Hardware Security Modules



- Afilias

- ◆ Dublin, Ireland (Horsham, PA)

- Registrar and DNSSEC provider



- Blue Cat Networks

- ◆ Toronto, Canada

- DNSSEC Appliance



Homeland
Security

DNSSEC Product Vendors - 2

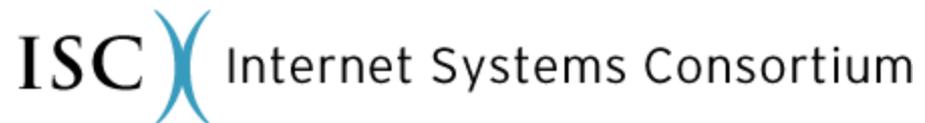
- Data Mountain Solutions, Inc.
 - ◆ Northern Virginia
 - Manage .GOV domain for GSA



- Infoblox
 - ◆ Santa Clara, CA
 - DNS Appliances



- Internet Systems Consortium (ISC)
 - ◆ Redwood City, California
 - Original developers of BIND



**Homeland
Security**

DNSSEC Product Vendors - 3

- Microsoft

- ◆ Redmond, WA

- Available in Windows Server 2008 R2 and Windows 7

The Microsoft logo is displayed in a bold, italicized, black sans-serif font.

- NLNet Labs

- ◆ Amsterdam, The Netherlands

- Open Source NSD software

The NLnet Labs logo features the word "NLnet" in a green, bold, sans-serif font, with "Labs" in a black, bold, sans-serif font below it. The background consists of a grid of binary code (0s and 1s) in a light green color.

- Nominum, Inc.

- ◆ Redwood City, California

- DNS and DNSSEC service provider

The Nominum logo features the word "Nominum" in a grey, sans-serif font, with a red dot above the 'i'. Below it, the tagline "Connecting Networks and People" is written in a smaller, red, sans-serif font.

Homeland
Security

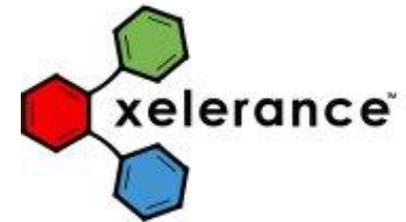
DNSSEC Product Vendors - 4

- Secure64 Corporation
 - ◆ Greenwood Village, CO
 - DNSSEC Signer Appliance
 - Funded by DHS S&T
 - Winner – Best of FOSE 2009



SECURE 64

- Xelerance Corporation
 - ◆ Ottawa, Canada
 - DNSSEC Appliance and Services



**Homeland
Security**

Drawbacks of DNS Security

- Increased complexity
 - ◆ Extra queries to create chain of trust
 - ◆ Resolvers must be able to verify digital signatures
- Increased zone database size
 - ◆ Contains more data
- Increased interaction between delegations
 - ◆ To secure delegations to sub-zones, or allow opt-ins
 - ◆ (Actually, this is a positive benefit)



Business Case Motivations

- **The bad guys ...**

- ◆ Increasingly **attacks are much more sophisticated**, highly motivated and resource rich.
 - Phishing and pharming attacks for \$.
 - Nation state attacks for military / intelligence goals.
 - Infrastructure attacks to “pull the rug from under” hardened hosts / services.



- **The good guys ...**

- ◆ Face **technical, economic, and political barriers** to deployment of some technologies.
 - Unregulated, low margin industry in the core of the network.
- ◆ Who pays for security? Who pays for insecurity?
 - Must have **incremental deployment** plan.
 - Must have **favorable / viable business model**.



**Homeland
Security**

DNSSEC Summary

- Domain Name System has vulnerabilities
 - ◆ Already being exploited, most recent demonstrations in Aug 2008
- Fixing it requires significant involvement with governments and private sector entities
 - ◆ ICANN, USG, Foreign governments, Domain owners, Domain Name Registrars
- There is a lack of customer “pull” for DNSSEC deployment
 - ◆ Government needs to set the example and we think we are doing that with OMB and GSA
- Still plenty of work to do



Douglas Maughan, Ph.D.
Program Manager, CCI
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170
<http://www.cyber.st.dhs.gov>



**Homeland
Security**

For more information, visit
<http://www.dnssec-deployment.org>



**Homeland
Security**

Resources

Reference:

- DNS and BIND, Albitz & Liu, O' Reilly & Associates
- FAQ: <http://www.nominum.com/getOpenSourceResource.php?id=8>
- BIND9 Administrator Reference Manual <http://www.bind9.net/manuals>

RFCs:

- <http://www.rfc-editor.org/>
- <http://www.ietf.org/>
- <http://www.dnssec.net/rfc>
- <ftp://ftp.ripe.net/rfc/>

Drafts:

- <http://www.ietf.org>
- <http://tools.ietf.org/wg/dnsop/>
- <http://tools.ietf.org/wg/dnsext/>
- <http://www.dnssec.net/drafts>
- <ftp://ftp.ripe.net/internet-drafts/>



Additional Resources

- <http://www.dnssec-deployment.org/>
- <http://www.dnssec.net/>
- <http://www.nlnetlabs.nl/dnssec/>
- <http://www.ripe.net/disi/>
- Papers from the 5th USENIX UNIX Security Symposium, Salt Lake City, Utah, June 1995
 - ◆ P. Vixie: DNS and BIND Security Issues
 - <http://www.usenix.org/publications/library/proceedings/security95/vixie.html>
 - ◆ S. Bellovin: Using the DNS for Break-ins
 - <http://www.usenix.org/publications/library/proceedings/security95/bellovin.html>



Related mailing lists

- DNS OARC: dns-operations@lists.dns-oarc.net
- IETF DNSOP: dnsop@ietf.org
- namedroppers@ops.ietf.org
 - ◆ DNSEXT IETF working group (DNS protocol development)
- techsec@ripe.net
 - ◆ RIPE Technical Security working group
- dns-wg@ripe.net
 - ◆ RIPE DNS working group



DNSSEC Initiative Resources

- DNSSEC Deployment Working Group
 - ◆ <http://www.dnssec-deployment.org>
 - ◆ Mailing list: dnssec-deployment@shinkuro.com
- NIST DNSSEC Project page
 - ◆ <http://www-x.antd.nist.gov/dnssec>
 - ◆ Links to NIST tools
- SPARTA DNSSEC Project page
 - ◆ <http://www.dnssec-tools.org>
 - ◆ Tools, Applications, Step-by-step guides.
- Secure Naming Infrastructure Pilot
 - ◆ <http://www.dnsops.gov>
 - ◆ Distributed test domain/training pilot

