What's Next in DNSSEC: Securing the Domain Name System (DNS)

FOSE 2010
Washington, DC
March 24, 2010

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

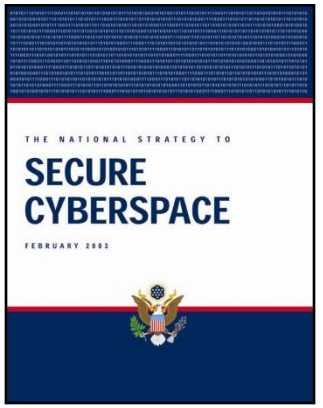
Homeland Security

Why are we here today?

- Update from last year's GovSec session
  - **The Keys to Deploying DNSSEC: Managing and Meeting Your OMB Domain Name System Requirements**
- Discuss Federal Government activities with DNSSEC
- Hear from those "Beyond Federal Government" – Early adopters
- Vendor Panel – Lessons Learned from Deployment with Government and other customers
- FOSE Exhibit Floor – DNSSEC Pavilion

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 – **DNSSEC Deployment Coordination Initiative**
  - **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
  - Outreach – web presence
- 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, blog, wiki
  - http://www.dnssec-deployment.org/
- Working with Civilian government (.gov) to develop policy and technical guidance for secure DNS operations and beginning deployment activities at all levels.
- Working with vendor community 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
  - Software Development
    - Server
    - Resolver
    - Applications
  - Operational Considerations
    - Root
    - Registries
    - Registrants
  - Measurement and Evaluation
  - Outreach and Training

Homeland Security

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

- Global ecosystem that benefits when all participate

- Registries
  - Work through various readiness levels
- Registrars
- ISPs
- Enterprise
  - Internal deployment as part of corporate system integrity and protection
  - Distinguish between safe and questionable sites

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

Homeland Security

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
    - Completed in January 2009
  - 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 Summary

- Domain Name System has vulnerabilities
  - Being exploited, most recent demonstrations in Aug 2008, Google Aurora
- 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 believe we are doing that with OMB and GSA
- Still plenty of work to do ….

Homeland Security

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

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

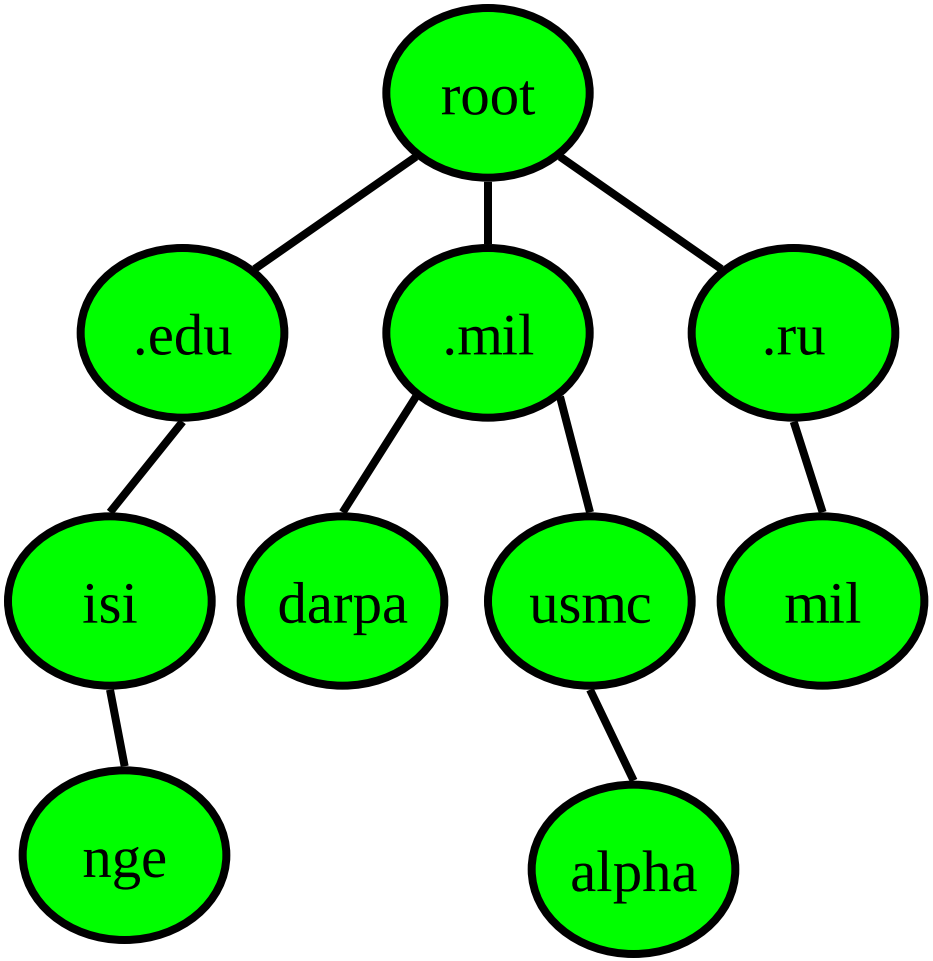
- DNS OARC: dns-operations@lists.dns-oarc.net
- IETF DNSOP: dnsop@ietf.org
- namedroppers@ops.ietf.org
  - DNSEXT IETF working group (DNS protocol development)
- techsec@ripe.net
  - RIPE Technical Security working group
- dns-wg@ripe.net
  - RIPE DNS working group

Domain Name System and Security

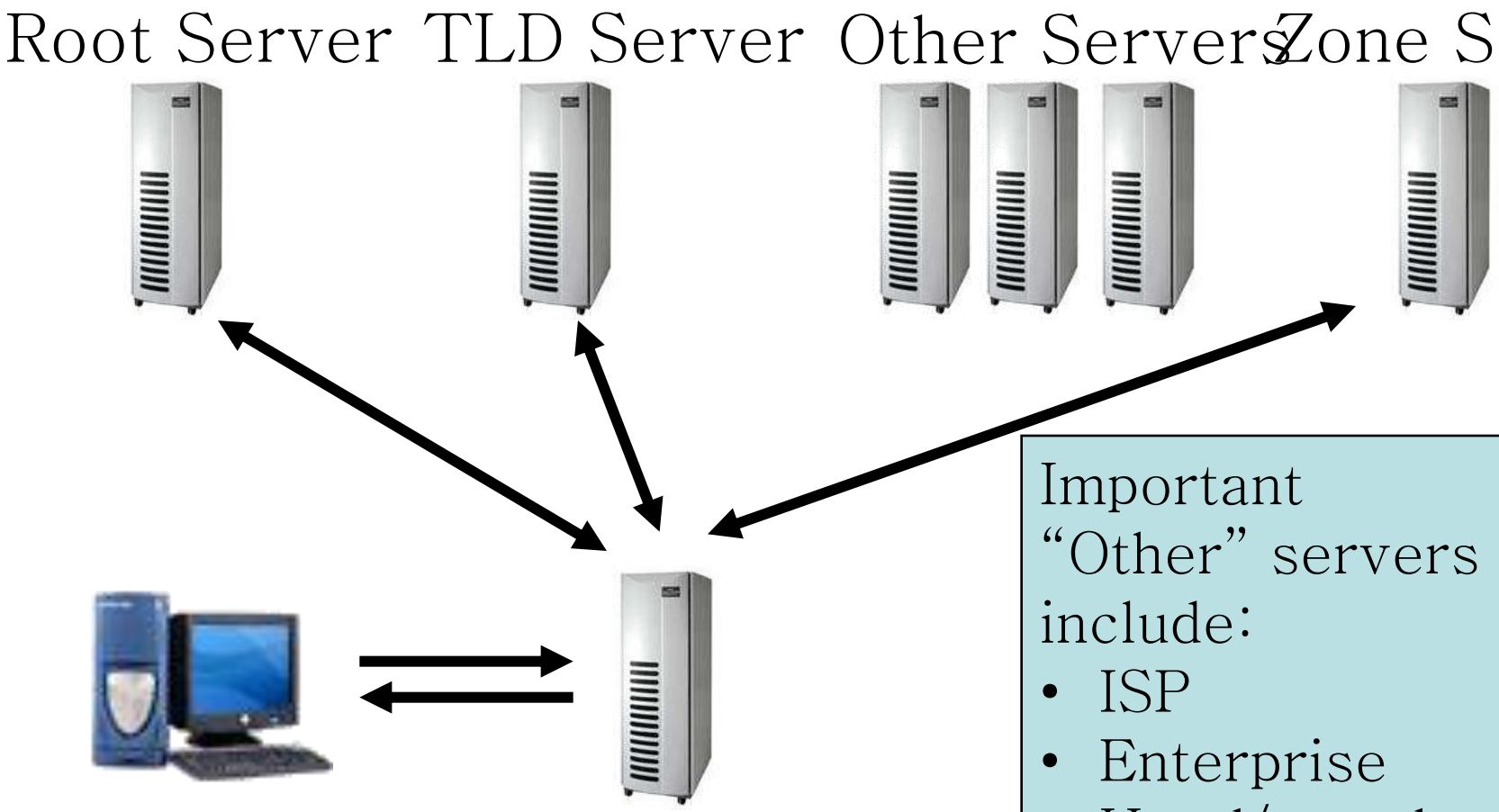
- Critical Internet infrastructure component
  - Virtually every Internet application uses the DNS
- DNS database maps:
  - Name to IP address
    - (for example: www.dhs.gov = **206.18.104.198**)
  - And many other mappings (mail servers, IPv6, reverse…)
- DNSSEC
  - Cryptographic signatures in the DNS
  - Assures integrity of results returned from DNS queries
    - Protects against tampering in caches and during transmission
  - End-system checks the chain of signatures up to the root

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



Important "Other" servers include:

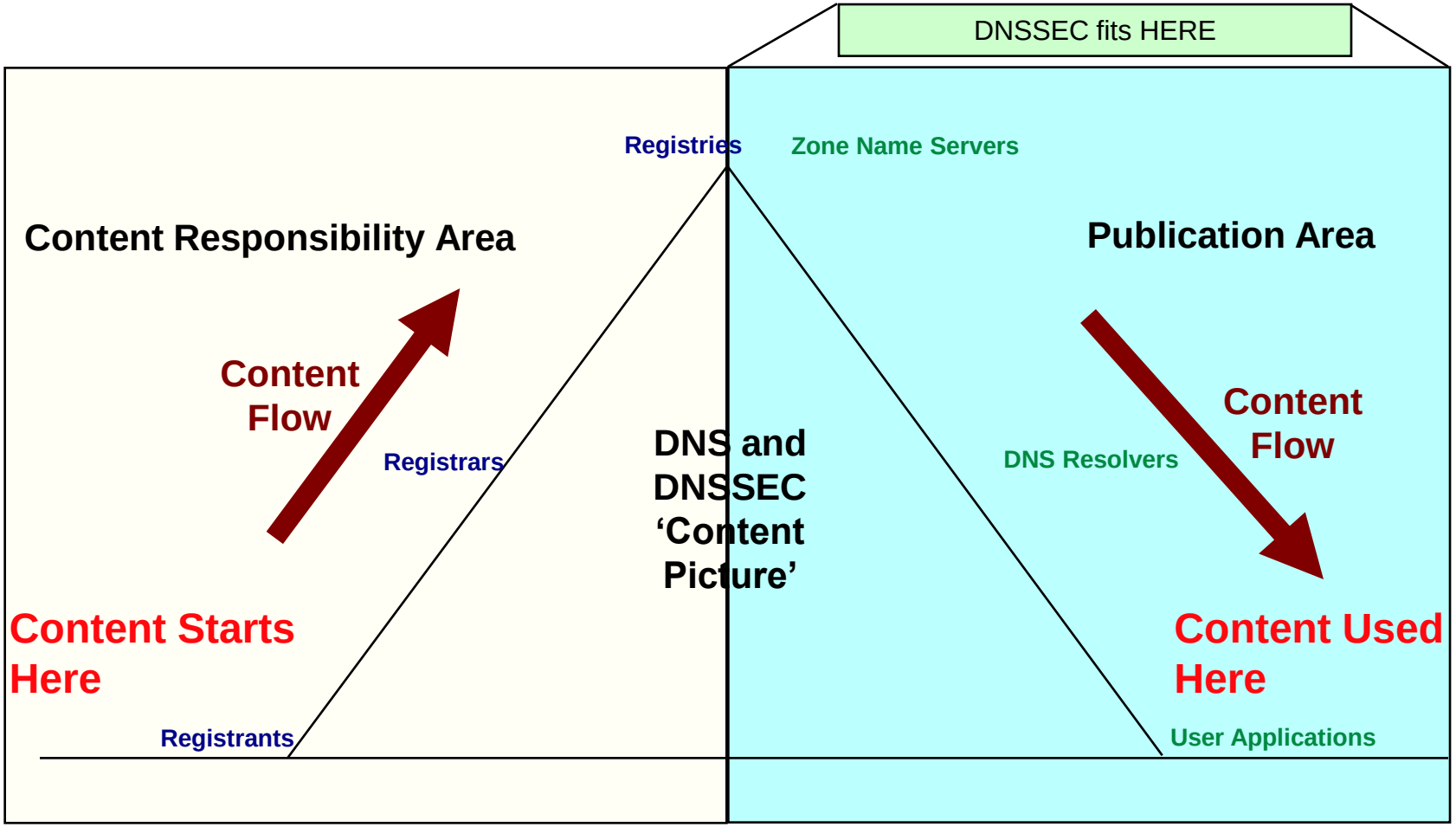
- ISP
- Enterprise
- Hotel/travel
- Public WLAN

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 and against the DNS are increasing
  - August 2008 – Kaminsky bug is a prime example
  - Attacks are becoming costly and difficult to remedy

Homeland Security

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



Homeland Security