Implementation of DNSSEC at BNL

John Bigrow
ITD Network Engineering
February 2, 2010

BROOKHAVEN NATIONAL LABORATORY

a passion for discovery

Office of Science
U.S. DEPARTMENT OF ENERGY

Topics

- BNL DNS Infrastructure Overview
  - What we have in place and why
- BNL DNSSEC Implementation
  - What we determined and did

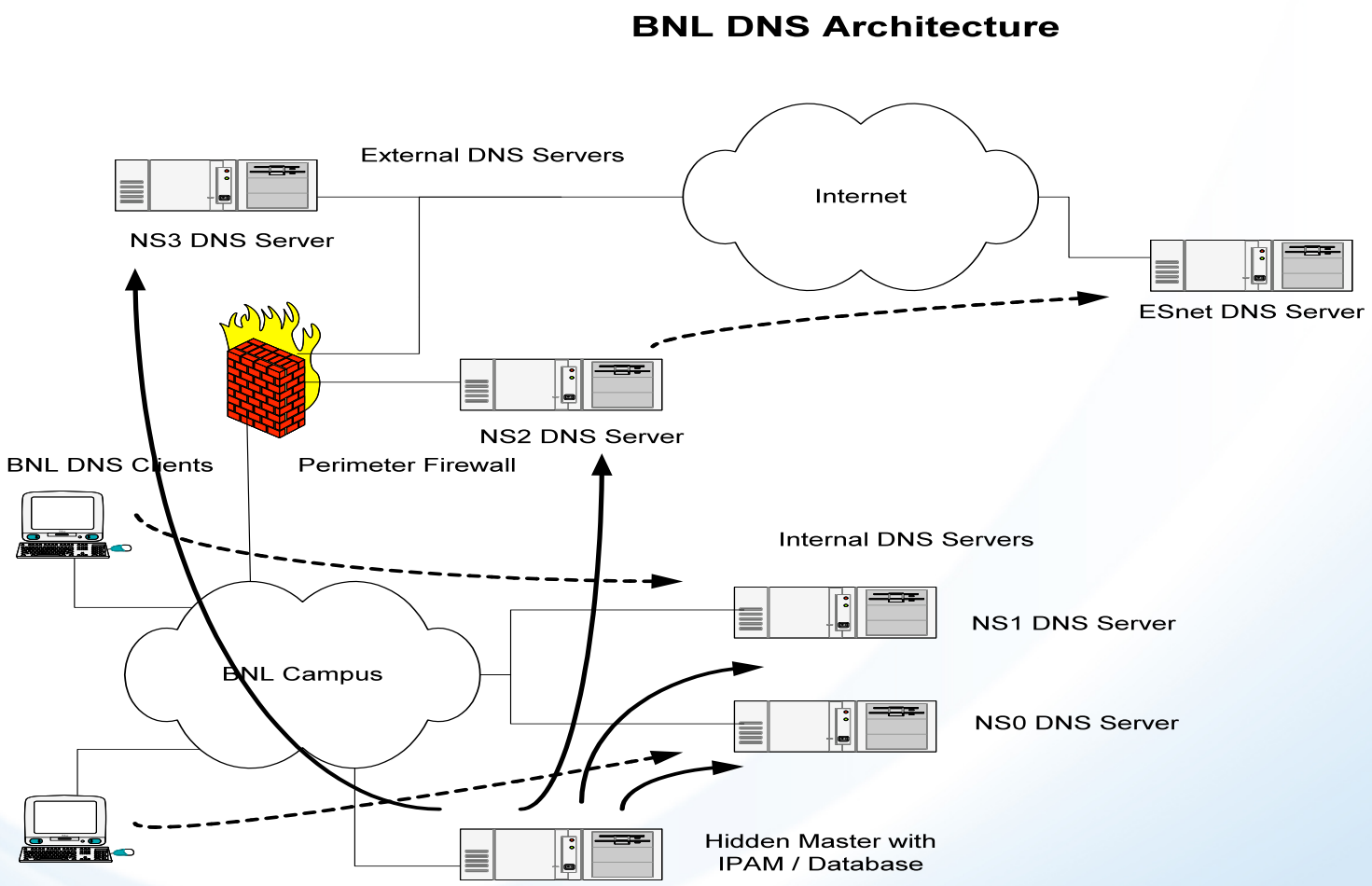
BNL DNS Infrastructure

- Split DNS architecture
- Using ISC BIND 9
- External – 2 BNL name servers + 1 ESnet name server
- Internal
- Provides Active Directory Services
- Visitor Network Servers use Limited Views

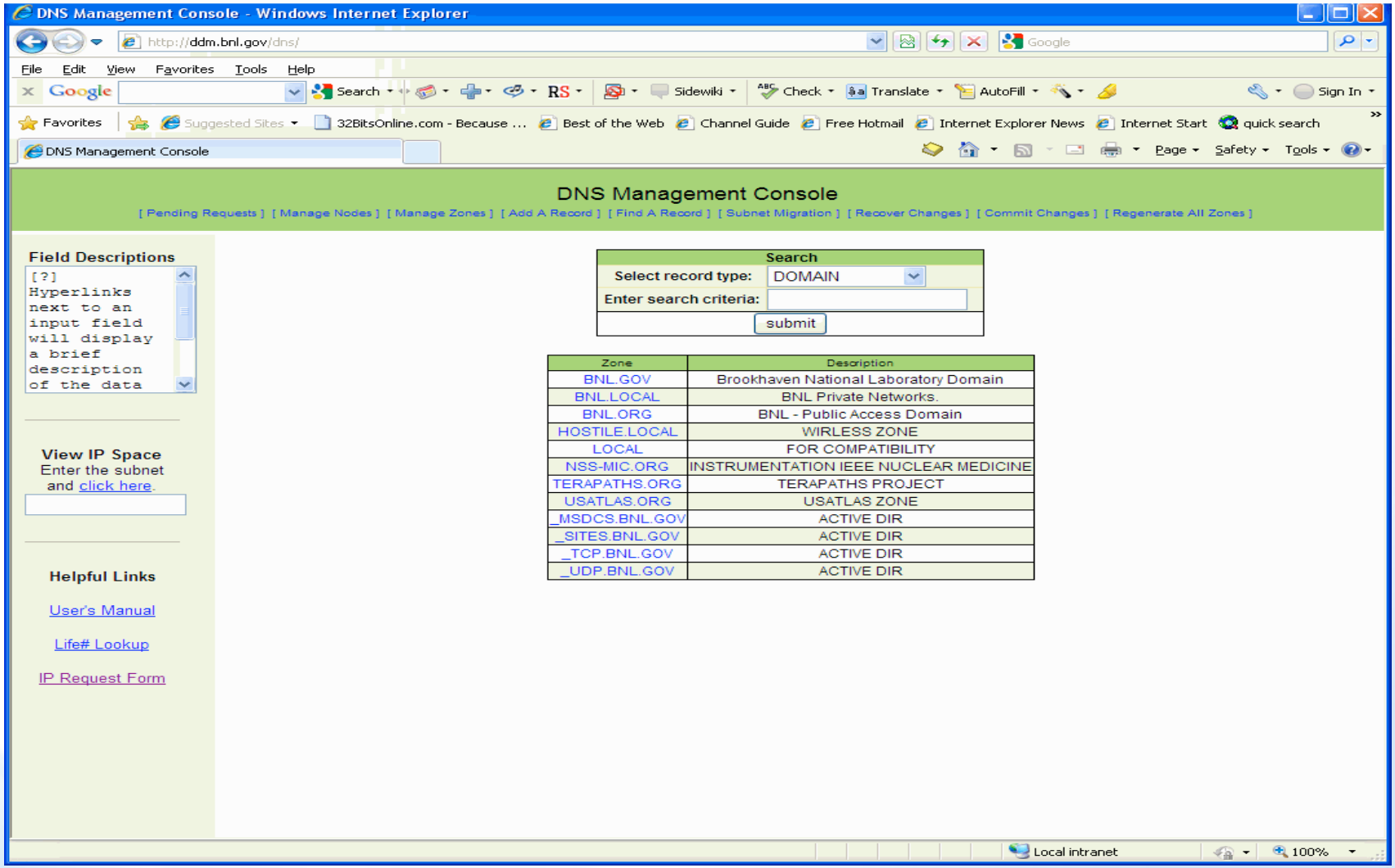
BNL DNS Infrastructure

- **Hidden master server for both internal and external DNS – DDM.BNL.GOV**
  - Web interface for IPAM (IP Address Management)
  - Oracle Database back-end
  - Integral Component of Campus Security Model
- **Set of name servers for:**
  - internal distribution layers • 6 total
  - external DNS • 2 BNL • 1 ESnet server (Registered)
  - visitor networks • 2 total
  - bnl.org • 2 total

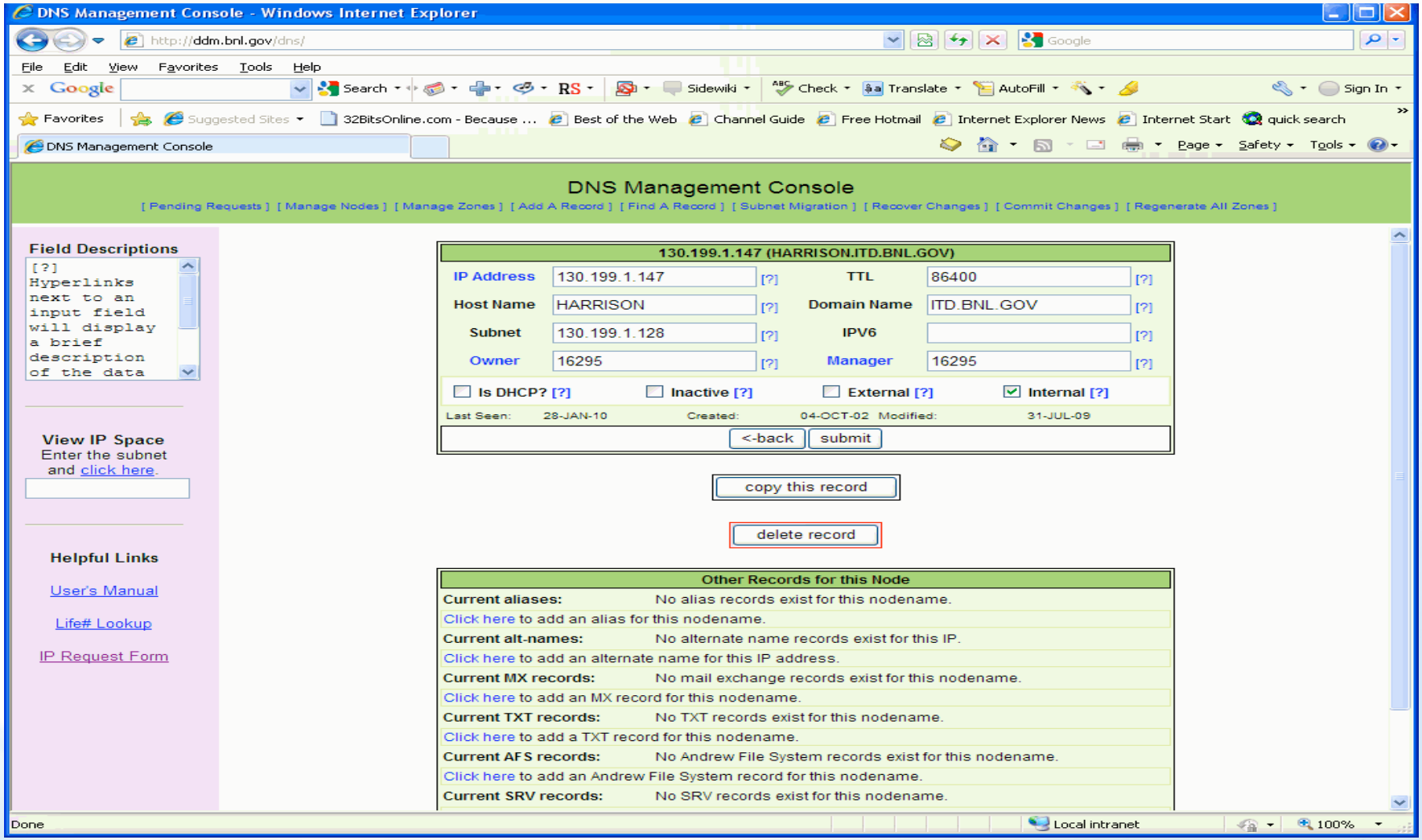
BNL DNS Infrastructure



BNL DNS IPAM


DNS Management Console - Windows Internet Explorer
http://ddm.bnl.gov/dns/
DNS Management Console
[Pending Requests] [Manage Nodes] [Manage Zones] [Add A Record] [Find A Record] [Subnet Migration] [Recover Changes] [Commit Changes] [Regenerate All Zones]
Field Descriptions
[?] Hyperlinks next to an input field will display a brief description of the data
View IP Space
Enter the subnet and click here.
Helpful Links
User's Manual
Life# Lookup
IP Request Form
Search
Select record type: DOMAIN
Enter search criteria:
submit
Zone | Description
BNL.GOV | Brookhaven National Laboratory Domain
BNL.LOCAL | BNL Private Networks.
BNL.ORG | BNL - Public Access Domain
HOSTILE.LOCAL | WIRLESS ZONE
LOCAL | FOR COMPATIBILITY
NSS-MIC.ORG | INSTRUMENTATION IEEE NUCLEAR MEDICINE
TERAPATHS.ORG | TERAPATHS PROJECT
USATLAS.ORG | USATLAS ZONE
_MSDCS.BNL.GOV | ACTIVE DIR
_SITES.BNL.GOV | ACTIVE DIR
_TCP.BNL.GOV | ACTIVE DIR
_UDP.BNL.GOV | ACTIVE DIR
Local intranet
100%

BNL DNS IPAM


DNS Management Console - Windows Internet Explorer
http://ddm.bnl.gov/dns/
DNS Management Console
[Pending Requests] [Manage Nodes] [Manage Zones] [Add A Record] [Find A Record] [Subnet Migration] [Recover Changes] [Commit Changes] [Regenerate All Zones]
Field Descriptions
[?] Hyperlinks next to an input field will display a brief description of the data
View IP Space
Enter the subnet and click here.
Helpful Links
User's Manual
Life# Lookup
IP Request Form
130.199.1.147 (HARRISON.ITD.BNL.GOV)
IP Address 130.199.1.147 [?]
TTL 86400 [?]
Host Name HARRISON [?]
Domain Name ITD.BNL.GOV [?]
Subnet 130.199.1.128 [?]
IPV6 [?]
Owner 16295 [?]
Manager 16295 [?]
Is DHCP? [?] Inactive [?] External [?] Internal [?]
Last Seen: 28-JAN-10 Created: 04-OCT-02 Modified: 31-JUL-09
<-back submit
copy this record
delete record
Other Records for this Node
Current aliases: No alias records exist for this nodename.
Click here to add an alias for this nodename.
Current alt-names: No alternate name records exist for this IP.
Click here to add an alternate name for this IP address.
Current MX records: No mail exchange records exist for this nodename.
Click here to add an MX record for this nodename.
Current TXT records: No TXT records exist for this nodename.
Click here to add a TXT record for this nodename.
Current AFS records: No Andrew File System records exist for this nodename.
Click here to add an Andrew File System record for this nodename.
Current SRV records: No SRV records exist for this nodename.
Done
Local intranet
100%

BNL DNS Infrastructure

- We are only signing the bnl.gov domain (for both internal and external instances).
- We are not performing DNSSEC validation for clients.
- We are rotating our ZSKs monthly, KSKs yearly.
- Record signatures are 7 days.
- We do not have dynamic DNS so all changes require a re-signing of the whole zone (after serial increment, of course).

BNL DNSSEC Implementation

Key management - Researched solutions

- **Appliances which will manage zones, autosign, maintain keys, etc.**
  - Total IPAM solution, our database is used by too many apps internally
- **DNSSEC freeware/open source tools**
  - Does not take split-DNS into consideration
  - Some require drastic changing of directory formats
  - Many in alpha or beta, not reliable
- **Bump in the wire (Secure64)**
  - Appliance which acts as master, real master xfers zone, appliance signs and xfers to rest
  - Expensive, requires certain type of hardware.

BNL DNSSEC Implementation

Key management – BNL solution

- **In house scripting of BIND signing binaries**
  - Scripts work in conjunction with current in-house IPAM solution
  - Scripts are portable, other Labs show interest
  - Combination of cron & scripts

- **Automation for any DNSSEC zone:**
  - Auto - ZSK & KSK generation
  - Auto - ZSK roll-over (KSK would be manual – but is only yearly)
  - Auto - Daily SOA incrementing and zone signing
  - Auto - Zone signing after zone modification

Thanks

- ESnet for providing off-site tertiary DNS
- ITD Unix Services
  - Server Management
  - Custom Scripting
- ITD Application Services
  - Wonderful IPAM solution

Final Questions/Comments?