DNSSEC at ORNL

Paige Stafford
Joint Techs Conference, Fairbanks
July 2011
Outline

• Background
  – Brief review of DNSSEC
  – ORNL before DNSSEC was implemented

• Implementation experience
  – Signer appliance
  – Validation

• Current DNSSEC status after more than a year

• Next phase of DNSSEC
Brief Review of DNSSEC

• Two distinct processes
  – Verification – refers to the source
  – Validation – refers to the records themselves

• Four New Types
  – DNSKEY
  – DS Record
  – RRSIG
  – NSEC
The DNSKEY

- DNSKEY -- Public crypto keys (2 types)
  - Key Signing Key (KSK)
    - Signs the keys of a zone
    - Public hash of this key is published in the parent as a DS record
  - Zone Signing Key (ZSK)
    - Signs records in the zone itself
    - Signed by the KSK
The DS Record

- **DS: Delegation Signer**
  - The public part of the zone’s KSK
  - Stored in the parent zone, and signed by the parent
    - E.g. "ornl.gov" DS record is found in the "gov" zone
  - Establishes “chain of trust” to **verify** source

---

The “ornl.gov” DS record resides in the “.gov” zone

```
# dig ornl.gov DS +trace  (or use @b.gov-servers.net)
<snip>
ornl.gov.   86400 IN   DS   28386 7 1 FCD201756C17E60C5EB0F1865E1AB1B5A6AE69D2
ornl.gov.   86400 IN   DS   28386 7 2 01AE09C91EEC9F97EE85158D6E0323FE94738CD3FC12DE0C7F3DC69B 9C21710B
gov.       172800 IN   NS   a.gov-servers.net.
gov.       172800 IN   NS   b.gov-servers.net.
;; Received 165 bytes from 209.112.123.30#53(b.gov-servers.net) in 40 ms
```
The RRSIG record

• **RRset** *(only in reference)*
  – unique set of [Name/Type]
  – Not a type of DNS record

• **RRSIG**
  – One for each RRset
  – Has expiration date!
  – **Validates** that the data can be trusted
Example RRSIG

# dig ornl.gov MX +dnssec +multiline

;; ANSWER SECTION:
ornl.gov.  14400 IN MX 10 emroute3.ornl.gov.
ornl.gov.  14400 IN MX 10 emroute4.ornl.gov.
ornl.gov.  14400 IN MX 10 emroute1.ornl.gov.
ornl.gov.  14400 IN MX 10 emroute2.ornl.gov.

ornl.gov.  14400 IN RRSIG MX 7 2 14400 20110730001315 ( 
  20110630070831 19471 ornl.gov.
  D9HsN3rlLrM1++CHycrYIb7IoF6r9iCKsbnGhn//MV/L
  +Sf+PxNRFjfbQDub48lNK4W/pW8AdbXAb8RR/W6X4itH
  Kgo+CQONko/BJY3K6+iOAkzWiH2iHwkK2h4W7hZUkBdW
  K6oKEaD0DbE1gmSSu5YZ8hD0bJbGjJrzK/gVdjg= )

RRset
All MX records for ORNL.GOV

Expiration date

Inception date

RRsig
Signed by the ZSK key
The NSEC record

- **NSEC** (or NSEC3) – stores any defined types for a given name
  - Validates the absence of a record
  - NSEC3 adds a layer of security onto the NSEC process
Before DNSSEC

- ns.ornl.gov slaved from hidden stealth
- ESNet slaved from ns.ornl.gov
DNSSEC Considerations

• DNSSEC motivated by OMB mandate
  – 2nd Level “.gov” domains signed (14)

• Network considerations
  – Firewalls modified to handle large DNS packets (UDP/TCP)

• Hardware considerations
  – Needed more CPU/Memory to handle increased load

• Software considerations
  – Sufficient (Bind 9) for both validation and handing out signed data
DNSSEC Considerations, Cont.

• Signer appliance needed

• Requirements:
  – Integrate into ORNL’s current IPAM system
  – Minimal effort (fully automated)

• Only two suited our infrastructure, both expensive
  – Xelerance and Secure64

• Only one had a web interface
  – Xelerance
Implementing Signing

- Introduced new server, NS0 (ns0.ornl.gov)
- New signer appliance and backup (hot spare)
  - Signer slaves from stealth to create new master
  - NS0 slaves from signer
- Easy Integration
  - Except…

![Diagram of External DNS Infrastructure]
One Issue Signing

• Separating unsigned from signed caused issues
  – All zones no longer on same server
  – Child delegation missing
  • Child domain queries had failed without explicit delegation (NS record)

\[
\text{e.g.}
\begin{align*}
\text{ccs.ornl.gov.} & : 3600 \quad \text{IN} \quad \text{NS} \quad \text{ns.ornl.gov.}
\end{align*}
\]
**ORNL’s Final External Setup**

- NS0 is currently slave with both signed and unsigned
- Two views on a single server
Implementing Validation (Internal DNS)

• Validating Server hardware upgrades
  – Especially CPU/Memory

• Started with the “.gov” trust anchor
  – Root wasn’t yet signed

• More monitoring of system usage
  – sar – monitors performance, resource usage
  – dnstop – helps to find dns client trouble makers
  – Load handled okay
Validation Issues

• Plagued by validation errors
  – Serious and numerous validation failures at first (Early 2010)
    • e.g. tganet.gov, pccotc.gov, twai.gov (dept. of Treasury)
  – DNS appears broken when query resolves outside

• Solution
  – Validation only for more secure enclaves only
  – Still finding a few validation errors per month
    • Notifying corresponding DNS admin…
  – Monitor failures and revisit
Who’s Validating Today?

• Only 8-10% validating
  – One study of how to best determine who is validating
  – Looked at who is validating .org from the root
  – “Observing DNSSEC Validation in the Wild” April 2011

• Comcast validating as of 10/18/2010
  – Moving customers to DNSSEC-validating recursive resolvers
    • On a voluntary basis
What to Monitor

• According to one study, the most common mistakes are expired, missing or bogus RRSIG records

• Possible causes of RRsig errors
  – Slaving from miss-matched masters
    • E.g. only one of the masters in list has signed data
  – Zone TTL is much larger than RRsig TTL
    • Consider unavailable master
      – Stale data rate based on SOA TTL
      – Cached data outlives RRsig expiry dates
ORNL A Year Later

• Appliance still functioning okay
  – Kernel panics occasionally (need hardware upgrade)

• Still scrutinizing validation

• Monitoring using DNSSEC Checker (nagios plugin)

• Want to sign the rest of the domains
  – No drive from OMB
  – 189 public domains remain to be signed
  – Expensive to expand licensing
Study DNSSEC Software Choices

• DNSSEC is maturing
  – root is signed
  – Plethora of information, code, tools, etc.

• Better and more choices of software
  – “Tool Guide Series on DNSSEC” by VeriSign 2010
    • http://net.educause.edu/ir/library/pdf/CSD5928.pdf
  – “A Review of Administrative Tools for DNSSEC”
    • http://www.iis.se/docs/DNSSEC-Admin-tools-review-Final.pdf
Today’s DNSSEC Signers
Both Commercial and Open Source (not a complete list)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product version reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueCat Networks</td>
<td>Proteus 3.0.2.19</td>
</tr>
<tr>
<td>Infoblox</td>
<td>Infoblox 5.0</td>
</tr>
<tr>
<td>InfoWeapons</td>
<td>SolidDNS 4.0</td>
</tr>
<tr>
<td>ISC</td>
<td>BIND 9.7</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Windows 2008 R2 (6.1)</td>
</tr>
<tr>
<td>OpenDNSSEC</td>
<td>OpenDNSSEC 1.1</td>
</tr>
<tr>
<td>Secure64 Software</td>
<td>DNS Signer 3.1</td>
</tr>
<tr>
<td>Xelerance</td>
<td>DNSX Secure Signer 1.1</td>
</tr>
</tbody>
</table>

“A Review of Administrative Tools for DNSSEC“
– Written by Andreas Nilsson, Certezza, Spring 2010
**DNSSEC Software Comparison**

by Andreas Nilsson

<table>
<thead>
<tr>
<th>Product</th>
<th>Findings by the test team</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueCat</td>
<td>Full-fledged IPAM system. Relatively easy to get started with configuring DNSSEC on existing BlueCat Adonis appliances managed by Proteus. No NSEC3 opt-out support might be negative for TLDs and registrars.</td>
</tr>
<tr>
<td>InfoBlox</td>
<td>Another appliance based full-fledged IPAM system. All major DNSSEC functionality is there and the UI is modern and intuitive.</td>
</tr>
<tr>
<td>InfoWeapons</td>
<td>InfoWeapons is mainly a DNS server but integrates with third party IPAM. The DNSSEC functionality works as expected but the UI was relatively difficult to navigate. The SolidDNS appliance is available as a virtual machine.</td>
</tr>
<tr>
<td>ISC (BIND)</td>
<td>All major DNSSEC features are implemented and BIND is actually used as a base in several of the other support products. For administrators already using the BIND CLI for DNS management there is no need to change for DNSSEC reasons. One drawback is that keys are stored in clear-text by default so an HSM is typically required. Plus for ability to use the same key for several zones.</td>
</tr>
<tr>
<td>Microsoft</td>
<td>No DNSSEC policy management, the complete key management process is handled manually via CLI. Integration into the DNS Server MMC UI would have been preferable. No algorithm selection and no NSEC3 support. These factors combined make larger deployments impractical. Plus for ability to use the same key for several zones.</td>
</tr>
<tr>
<td>OpenDNSSEC</td>
<td>OpenDNSSEC is a CLI-based thin DNSSEC signer and is the most light weight solution reviewed. The SoftHSM feature comes in handy for smaller deployment scenarios. Currently a third party name server is required for outgoing zone transfers. The architecture is Linux like with opportunities to plug in third party tools or own scripts.</td>
</tr>
<tr>
<td>Secure64</td>
<td>Appliance based DNSSEC signer which can also work as a DNS server. All major DNSSEC functionality is there. A web UI would have been nice to complement the CLI but a plus for the security focus with a dedicated hardened OS and TPM key storage.</td>
</tr>
<tr>
<td>Xelerance</td>
<td>Appliance based DNSSEC signer which implements the major DNSSEC functionality. However the UI is non-intuitive and old fashioned which brings down the overall impression.</td>
</tr>
</tbody>
</table>
## Comparison of Open Source Signers

### VeriSign Study (2010)

<table>
<thead>
<tr>
<th>Features</th>
<th>BIND9.6</th>
<th>OpenDNSSEC</th>
<th>ZKT</th>
<th>DNSSEC-Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support PKCS#11 interface with an HSM</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic key generation</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Denial of existence using NSEC or NSEC3</td>
<td>●</td>
<td>●</td>
<td></td>
<td>(ZSK only)</td>
</tr>
<tr>
<td>Automatic key rollover</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Manual key rollover</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>(ZSK only)</td>
</tr>
<tr>
<td>Supported on Windows-based operating systems</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Supported on *nix-based operating systems</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Extraction of Delegation Signer (DS) records for publishing KSK to parent zone</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
</tbody>
</table>

- **ISC Bind v.9.7 more Automated**
  - Seamlessly integrated
  - Can sign zones transferred in via AXFR.
  - Fully automatic
  - XML configuration
  - HSM or SoftHSM
- **DNSSEC Zone Key Tool (ZKT)**
- **DNSSEC-Tools**

AFNIC Problems with Open Source

• AFNIC registry operates 6 ccTLDs (fr/re/pm/tf/wf/yt).
• NSEC3 records missing – ISC bug fixed immediately
• HSM unreachable, and home-grown code didn’t check for it

“Key Deletion Issues and other DNSSEC stories”

June 22th, 2011 vincent.levigneron@afnic.fr

• OpenDNSSEC is only used for Key Management.
• AEP Keyper HSM are used for Key storage.
• Bind (auto-dnssec allow; option set) do all the signature stuff (with HSM).
  – Version 9.7.1-P2 was first used.
  – Version 9.7.3 deployed after second outage.
• Homemade synchronization script to create V1.3 Bind key files from ODS data.
Signer Options Conclusion

• Three practical choices
  – Xelerance -- Currently in use
    • Purchase yearly licensing and new hardware
    • Cannot manage hardware ourselves
  – Bind 9.7+
    • Well understood by ORNL’s admin, existing hardware
    • Build wrapper around signing process – Moderate effort
    • No HSM
  – OpenDNSSEC
    • New Code, moderate learning curve, existing hardware
Overall Conclusion

• Requiring validation for all of ORNL is still a question

• For DNSSEC to succeed service providers must enable validation
  – Fall back to COTS

• Open-Source software is our next logical direction
Questions?