Assessing and Improving the Quality of DNSSEC Deployment

Casey Deccio, Ph.D.
Sandia National Laboratories

AIMS-4
CAIDA, SDSC, San Diego, CA
Feb 9, 2012

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.
Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions
DNS Security Extensions (DNSSEC)

- RRsets signed with zone’s private key(s)
- Signatures covering RRsets returned by server as RRSIGs
- Public keys published in zone data as DNSKEYs
- Resolver validates response
  - If authentic: Authenticated data (AD) bit is set
  - If bogus: SERVFAIL message is returned
Scalable authentication via a chain of trust

- DNSKEY must be authenticated
- Resolver must have some notion of trust
- Trust extends through ancestry to a trust anchor at resolver
- DS resource record – provides digest of DNSKEY in child zone
Backwards compatibility… kind of

- If no secure link exists between parent and child, referring (parent) server must prove non-existence of DS RRs
- NSEC/NSEC3 resource records provide authenticated denial of existence
- Child zones of insecure delegations may be unsigned or signed ("islands of security")
DNSSEC validation status

- **Secure** – unbroken chain from anchor to RRset

(Image from http://dnsviz.net/)
DNSSEC validation status

- **Insecure** – chain that securely terminates (i.e., insecure delegation)

(Image from http://dnsviz.net/)

Secure chain termination
DNSSEC validation status

- **Bogus** – broken chain

(Image from http://dnsviz.net/)
Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions
DNSSEC Maintenance

- RRSIG refresh
- DNSKEY rollovers
  - ZSK rollovers – non-SEP (secure entry point), self-contained
  - KSK rollovers – SEP requires interaction with parent or trust anchor
- Algorithm changes
DNSSEC Misconfiguration

- **DS Mismatch** – No DNSKEY matching DS in parent zone
- **DNSKEY Missing** – DNSKEY not available to validate RRSIG
- **NSEC Missing** – NSEC RRs not returned by authoritative server
- **RRSIG Missing** – RRSIGs not returned by some servers
- **RRSIG Bogus** – Signature in RRSIG does not validate
- **RRSIG Dates** – Expired or premature RRSIG dates
DNSSEC is hard.
Jan 10, 2012 – Comcast turned on DNSSEC validation for all its residential customers.

http://blog.comcast.com/2012/01/comcast-completes-dnssec-deployment.html
Jan 18, 2012 – Comcast customers could not access nasa.gov.

http://nasawatch.com/archives/2012/01/comcast-blocks.html
Jan 22, 2012 – Comcast customers could not access bitcoinica.com.

http://www.reddit.com/r/Bitcoin/comments/orzpq/attention_comcast_users_we_have_been_censored/
Comcast is *clearly* “censoring” these sites. But why?

Enter DNSViz…
DNSViz

- Actively monitors domains from single vantage point
- Makes results available for visual analysis at http://dnsviz.net/
But, they “fixed” it…
Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions
DNSSEC deployment survey

- Polled ~2,700 production signed zones over a year time frame (May 2010 – July 2011)
- Validation of SOA RR analyzed several times daily, anchored at ISC DLV or root zone (after July 2010 root signing)
- Identified maintenance and misconfigurations
Survey breakdown by TLD

The chart shows the number of zones and zones with misconfiguration for different TLDs. The TLDs are listed on the x-axis, and the number of zones is on the y-axis. The TLD 'gov' has the highest number of zones, followed by 'cz', 'org', 'arpa', 'net', 'edu', 'com', 'br', 'se', 'dk', 'de', 'be', and 'Other'.
RRSIG lifetimes

CDF
0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1

Days
0 30 60 90 120 150 180 210 240 270 300 330 360

RRSIG(DNSKEY) all zones
RRSIG(DNSKEY) zones with expired RRSIG

Sandia National Laboratories
## DNSKEY rollovers

<table>
<thead>
<tr>
<th>Key role</th>
<th>Zones that did not roll key (0)</th>
<th>Zones that rolled key once (1)</th>
<th>Zones that rolled key more than once (&gt;1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZSK</td>
<td>37%</td>
<td>11%</td>
<td>52%</td>
</tr>
<tr>
<td>KSK</td>
<td>72%</td>
<td>17%</td>
<td>10%</td>
</tr>
</tbody>
</table>
DNSKEY lifetime

KSK lifetime
ZSK lifetime
KSK lifetime (zones w/ bad rollover)
Misconfigurations by type

- DS Mismatch
- DNSKEY Missing
- NSEC Missing
- RRSIG Missing
- RRSIG Bogus
- RRSIG Dates

Legend:
- Incremental
- Partial
- Complete
Event duration

[Graph showing event duration over time with various line colors representing different types of mismatches and missing records.]
Repeat offense rate

- DS Mismatch
- DNSKEY Missing
- NSEC Missing
- RRSIG Missing
- RRSIG Bogus
- RRSIG Dates
IPv6 analysis

sandia.gov
(2012-01-18 22:18:28 UTC)
IPv6 inconsistencies

va.gov
(2011-12-15 03:21:39 UTC)
Outline

- DNSSEC protocol review
- DNSSEC maintenance and misconfiguration
- DNSSEC survey and results
- Conclusions and solutions
Summary of Observations

- Resolver operators are learning about third-party DNSSEC misconfigurations from their customers.
- Administrators aren’t detecting and correcting their DNSSEC problems in a timely fashion.
- Administrators aren’t learning from past mistakes.
Solutions

- Tools for DNSSEC comprehensive analysis
  - Hierarchical analysis (chain of trust)
  - Dependency analysis (CNAME, MX, NS, etc)
  - Server consistency analysis
  - Pointers to specification
  - Resources for corrective action
- Tools/resources for detection/notification of misconfiguration
  - Individual monitoring and alerts
  - Global monitoring and alerts
DNSViz – future plans

- Expansion of detailed analysis
- Passive monitoring, in addition to active monitoring
  - Diverse backend support
    - e.g., ISC Security Information Exchange (SIE)
  - Prioritized active probing
  - Alerts of misconfiguration
- RESTful API for programmatic third-party monitoring
- Cache analysis/local perspective
- Availability of software for diverse uses
Questions?

- ctdecci@sandia.gov