DNSSEC Monitoring

On a Shoe String
Monitoring

- **Why:** DNSSEC needs maintenance
  - Not an “install and forget” application

- **Why:** I’m Curious
  - How well is it done?

- **What:** Check just TLDs
  - Let’s start small

- **How:** Easy and Cheap
1. Find DNSSEC signed TLDs

   cat root zone | grep "IN   DS" | awk '{print $1;}' | sort -u > $tldlist

2. Validate these domains

   unbound-host -t SOA $tld

3. Notify by error

   echo $tld is bogus | mail jaap

4. Schedule using cron
Results

• ± 500 mails since January 2012
• Lot’s of repeats:
  • 400 for one ccTLD
• ± 30 different TLDs
• most for ccTLDs
# Hall of Shame

<table>
<thead>
<tr>
<th>TLD</th>
<th>TLD</th>
<th>TLD</th>
<th>TLD</th>
<th>TLD</th>
</tr>
</thead>
<tbody>
<tr>
<td>xn--llacc</td>
<td>mm</td>
<td>bw</td>
<td>xn--kpry57d</td>
<td>xn--mgbx4cd0ab</td>
</tr>
<tr>
<td>ad</td>
<td>lat</td>
<td>kg</td>
<td>alsace</td>
<td>xn--6qq986b3xl</td>
</tr>
<tr>
<td>xn--3bst00m</td>
<td>zm</td>
<td>xn--80aswg</td>
<td>xn--80asehdb</td>
<td>mil</td>
</tr>
<tr>
<td>wme</td>
<td>trade</td>
<td>sx</td>
<td>repair</td>
<td>nyc</td>
</tr>
<tr>
<td>land</td>
<td>ke</td>
<td>feedback</td>
<td>club</td>
<td>ch</td>
</tr>
<tr>
<td>ceo</td>
<td>cancerresearch</td>
<td>biz</td>
<td>bargains</td>
<td>az</td>
</tr>
</tbody>
</table>
Error types

• Expired Signatures
  • Oops!

• Non matching algorithms
  • Botched roll-overs

• Missing signatures
  • Sloppy operation

• SERFAIL
By TLD type

- Mostly ccTLDs
  - repeated failures

- (g)TLDs
  - software/network problems?

- “new” gTLDs
  - single failures on startup
What now?

• Lazy Monitoring is easy
  • Ripe’s DNSmon started like this (mail jaap on error)

• Long term monitoring shows possible trends

• Turn this into a service?
  • Contact <jaap@NLnetLabs.nl>
Other DNSSEC Tools

• Rick Lamb’s Early Warning system
  • www.dnssek.info

• DNSSEC checkers
  • dnssec-debugger.verisignlabs.com
  • dnsviz.net
  • zonemaster.se