DNSSEC Monitoring

On a Shoe String

NLnet Labs

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

Methodology

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

xn--l1acc	wme
mm	trade
bw	sx
xn--kpry57d	repair
xn--mgbx4cd0ab	nyc
ad	land
lat	ke
kg	feedback
alsace	club
xn--6qq986b3xl	ch
xn--3bst00m	ceo
zm	cancerresearch
xn--80aswg	biz
xn--80asehdb	bargains
mil	az

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

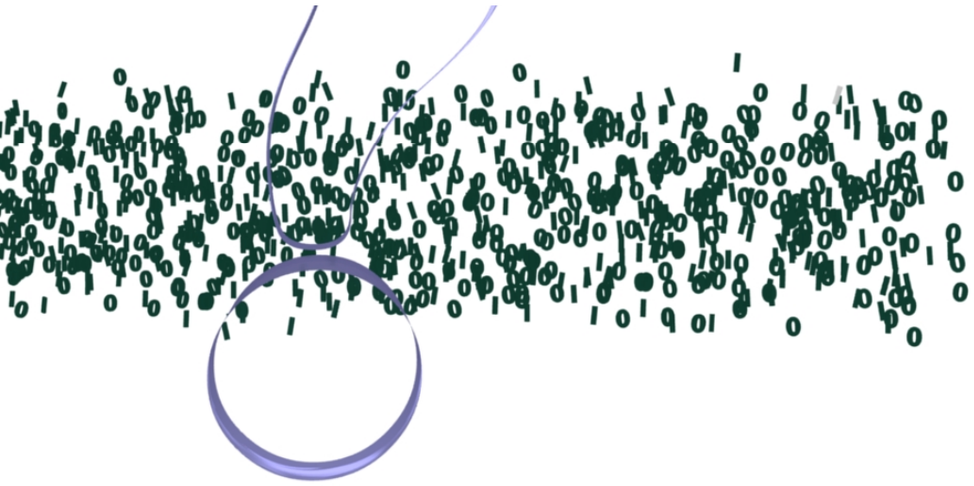
What now?

- 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



Questions

NLnet Labs