DNSSEC in a small ccTLD

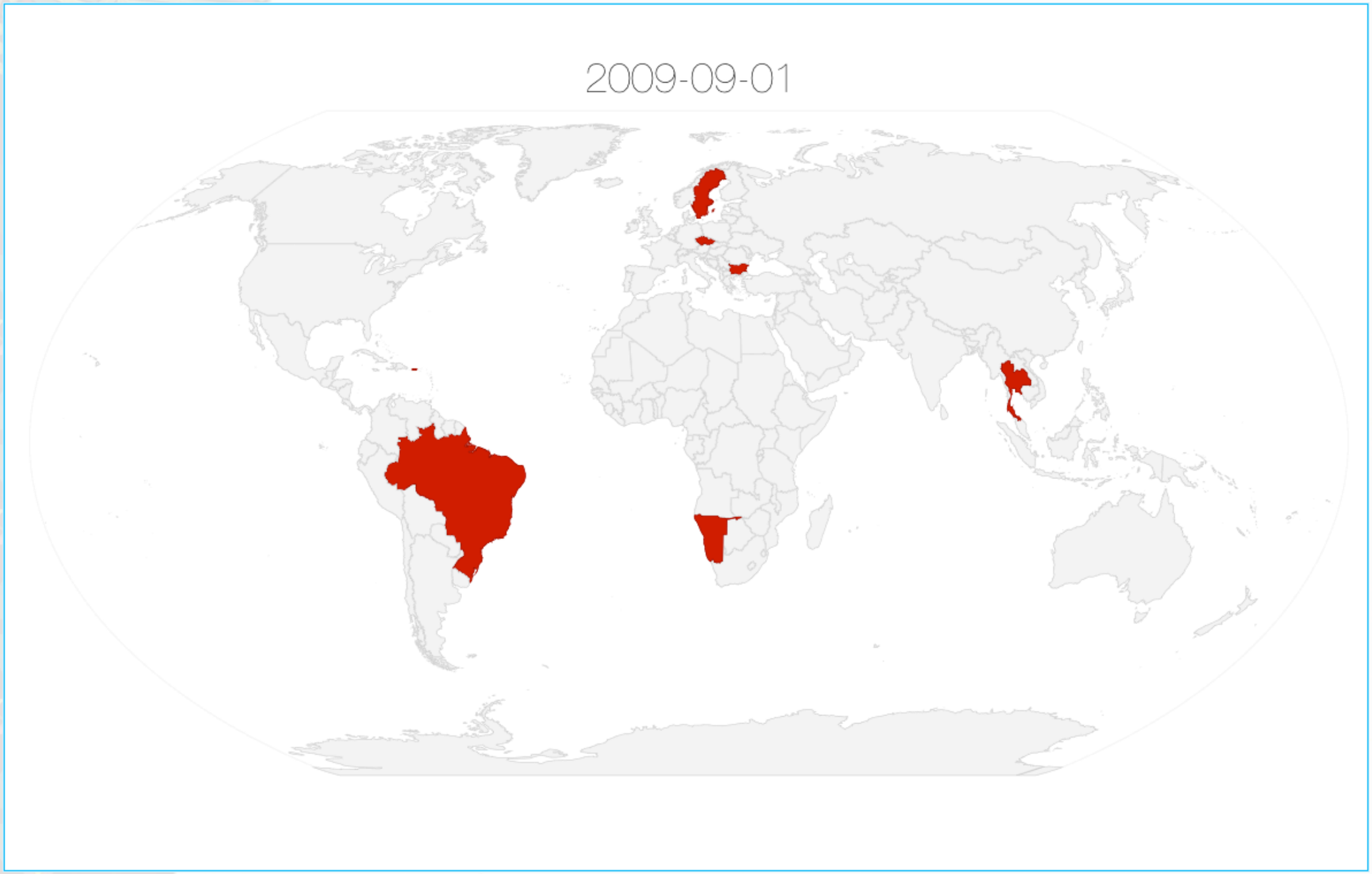
Dr Eberhard W Lisse

Namibian Network Information Centre (cc)

2009-10-26

Copyright © 2009 NA-NiC

DNSSEC



Why?

Because!

- It can be done.
- It should be done.
- I wanted to do it!

How Did We Do It?

- Ubuntu
  - 8.04.2 LTS (Server Edition)
  - Firewall
  - Serious Redundant Backup
- CoCCATools

  Automated Zone Generation
- Provisioning Script (Perl)

Key Generation

dnssec-keygen -r /dev/urandom -a RSASHA1 -b 1024 -n ZONE na

Kna.+005+19392.key

Kna.+005+19392.private

dnssec-keygen -r /dev/urandom -a RSASHA1 -b 4096 -n ZONE -f KSK na

Kna.+005+24484.key

Kna.+005+24484.private

Entropy

- /dev/random
  - truely random
  - may block
    - Hardware
    - OS X
- /dev/urandom
  - less random
  - doesn’t block

Provisioning

- .NA
  - sign Zone File (BIND9 Tools)
  - scp Zone File to Primary
    - Primary picks up and reloads regularly
- Second Levels
  - unsigned (at present)
  - copy over to BIND directory (Hidden Primary)
  - reload BIND

coccaprovision.pl

- CoCCATools dumps Zone Files regularily
  - admin.zones.2009.10.20.0900.zip
- Compare the last two ZIP for size
  - Terminate if size suspect (and email error)
  - Unzip otherwise
- Copy stub zone files to BIND directory

coccaprovision.pl

- Read Zone File (into memory)
- Write to Intermediate File
- Append to Intermediate File:

```
print $IF <<EOF;
    \$INCLUDE Kna.+005+24484.key
    \$INCLUDE Kna.+005+19392.key
EOF
close($IF);
```

coccaprovision.pl

Do the Deed

```
$zserial  = "KEEP"

$zoptions = "-o na -N $zserial";     # origin

$zsfile   = "-f na.zone.signed";

$zifile   = "na.zone.zs";

$zsigner  = "/usr/sbin/dnssec-signzone";

$zonesign = "$zsigner $zoptions $zsfile $zifile";
```

coccaprovision.pl

- back up NA.domain on the primary
- scp na.zone.signed to the primary
- rename na.zone.signed to NA.domain
- clean up local temp files
- Send email

coccaprovision.pl

- reload local BIND

  Hidden Primary for the sub zones

  Triggers AXFR from Secondaries

- exit
- Primary reloads (NA.domain) regularily

  Keeps previous backups

  Easy Rollback (manual)

Lessons Learned

- RTFM!

  Those Abbreviations...

- Lawrie's Laws:

  If it Works on the First Attempt, there is Something Seriously Wrong!

  You Don't Need to Hire a Consultant, a Friend on the Other End is All you Need!

- Hide the Key!

- Or Don't!

Thanks

Jeremy Hitchcock (DynDNS)

Peter Losher (ISC)

Bill Semich, Daniel Pouzzner (.NU)