DNSSEC in NL
Testbed #2

Jaap Akkerhuis

Summary

Players

DNSSEC 101

Testbed #1

Testbed #2: SECREG

  Goals

  Set up

  Lessons learned

Future

Players

SIDN

Registry for NL

Bart Boswinkel

Yours truly

NLnetlabs

Research arm of NLnet foundation

Miek Gieben

Ted Lindgreen

DNSSEC 101

What DNSSEC *does not*

  Secure the internet

  Create a PKI

  Encrypt the IP layer

  Secure IP rights, such as © Ⓟ ®

    IP != IP™ lawyersˢᴹ

DNSSEC *does*

  Authenticate queries

  Allow spoofing detection

DNSSEC 101 (2)

Why DNSSEC?

Trace to trusted source

Helps to deploy security protocols

IPsec

PKI

Raises quality of zone data

Authenticate denial of existence

Wild cards are hard!

Testbed #1

Operational done in a shadow tree: nl.nl

Classic RFC 2535

Crypto too expensive?

   Not

Key signing too hard

  Yes

     Sig@Parent → DS record

New RFC's: DNSSEC-bis

Testbed #2: Goals

Hands on operational experience
What can be automated?
Impact on registry, registrar, registrant

Testbed #2 Operation

Separate "secure" registry: SECREG

Separate name servers

  Allows registrars to play

    Registrants as well

      and users?

Two Servers in nl, one in se

  One recursive

Limited lifetime (Yr 2003)

Testbed #2

Zone signed every day

   1½ Hour (800K domains, 1.8M Records)

Size

   350MB Zone file

   15 Minutes loading time

One DS per secured zone

   (One KSK)

One operational Problem

SECREG Operations

Securing a domain

  Getting the KSK signed

Key rollover

  Replacing existing key

Block

  Revoke security (back to normal)

    Key compromise
    Administrative reasons

SECREG Registrars

Registrar #1
  Production system
   15000 domains
      Same key for all
Registrar #2
  140 domains
      Different keys

Findings

No problem with
- Signing
- Serving
- Zone size
- Key rollover

Lot's can be automated

Findings

Contact role needed

    Zone contact, signs updated zone file

Distributing Registry key

    Not needed when root is signed

More emphasis on security

Handling of key compromises

Findings

When not to do DNSSEC

    Weak existing authentication of registrars or registrants

Too bold expectations

    such as dnssec secures

        the network

        ...

Useful links

The full report:

    www.secreg.nlnetlabs.nl

Lots of links to DNSSEC material:

    www.dnssec.net

Questions

????

at sidn.**nl**