32nd public ICANN meeting

Productive DNSSEC deployment

Lutz Donnerhacke

DNSSEC 1.6.5.3.7.5.1.4.6.3.9.4.e164.arpa.
OpenPGP 1C1C 6311 EF09 D819 E029 65BE BFB6 C9CB

IKS

Productive DNSSEC deployment

History

- Late adopter: Use existing tools. *Thank you!*
- Starting with a DLV, resulting in a survey
- Deploying DLV to ISP core and own company
- Introducing a signed root (on IANA zone data)
- Deploying signed root to customers
- Large scale test bed: bgp.arpa.
- Provide tools for others (due to customer request)

IKS

Productive DNSSEC deployment

Requirements

- Stable software
- Fully automatic key management
- Skilled customer hotline
- Upper management commitment
- Enthusiastic techies to solve obscure problems
- No sales activities: no customer expectations

Productive DNSSEC deployment

Hard lessons

- Resign everything, every time, automatically:
  - Expired RRSIG on NS for the root zone required a bicycle ride on Christmas 2006
- Don't give up on DNSSEC „caused“ errors
  - EDNS0 responses dropped by firewalls
  - Email can't be received from qmail-MTAs
  - Admins will complain about broken tool chains

IKS

Productive DNSSEC deployment

Summary of two years experience

- Customers *feel* more secure or do not notice
- Understanding of in house zone data *generation*
- Sometimes configuration errors where detected
- Train people is the time consuming and hard
- There is no ROI in DNSSEC, it's infrastructure
- Leaving customers face problems in the first days

IKS

Productive DNSSEC deployment

Large Scale Deployment

- IETF draft: securing BGP with DNSSEC
- bgp.arpa test bed simulating the RIPE region:
  - ~30000 zones with ~3G (1G compressed) data
  - Resigning takes about 3 days, heavy use of make
  - Misusing a „private webserver“ running Tomcat ...
  - 260 instances of nsd on 256MB 2GHz Celeron

Productive DNSSEC deployment

Interactive DNSSEC checker

- Ajax based website demonstrating DNS lookups
- Using multiple (signed) roots and DLVs
- Click to mount pharming and poisoning attacks
- Demonstrate when and how DNSSEC can help
- Still under development: Ideas welcome

http://www.iks-jena.de/cgi-bin/dnssec_how_dns_works.pl

Productive DNSSEC deployment

Questions?

Signed answers.

IKS