Improving the resilience of DNS

ENISA – Athens

Productive DNSSEC environments

Lutz Donnerhacke
IKS GmbH, Jena

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

Relevant company history

DNSSEC activities

- Late adopter: Not developing the protocol
- 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 tests: bgp.arpa.

IKS

Productive DNSSEC deployment

Requirements

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

IKS

Usage scenarios

Signing

- Admins complain about broken (old) tool chains
- Zone different in various views (RFC1918/NAT)
- Automatic resigning requires additional daemons, additional monitoring, and additional alarm plans
- Signing while zone is modified: broken zone
- DNS appliance without DNSSEC capabilities

→ Remote signing tools using hidden primary

IKS

Usage scenarios

Verifying resolvers

- Turing on verification is useless
- Maintaining distributed trust anchors is hard
- Central maintaining is easier: DLV/signed root
- DLV caused software problems (mostly solved)
- Signed root misses important TLDs
- Security aware companies maintain own TARs

IKS

Usage scenarios

Benefits or ROI

- Storage of public keys: Use DNS as PKI for SSH (automatic), OpenPGP and X.509 (manual)
- Securing ENUM
- Banks fear legal consequences if not all possible protection is offered
- Spam avoidance: Securing DKIM etc. pp.
- DNS as distributed database: bgp.arpa

Open discussion

Who is really using DNSSEC?

- For which purpose?
- Which area of impact? LAN, company, or global?
- Does it work automatically? Out of the box?
- Which trust anchor management is used?
- Does it open new problems? Privacy?
- How was is done before/without DNSSEC?
- Is DNSSEC a product or plain (and free) infrastructure?

IKS

Productive DNSSEC

Questions?

Signed answers.

IKS