Latest developments in DNSSEC

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
NSEC3 is coming

NSEC3 becomes popular

• .GOV and .ORG are going to NSEC3
• .GOV put the first real implementation online
• Causes a lot of software problems
• Validating errors can't be ignored anymore
• Huge step forward: NSEC3 is ready to use
• .DE starts testbed with NSEC3
Commercial interest

Money starts flowing

- Companies offering DNSSEC go to public
- Start of regular, commercial services
- Targeting to governmental institutes and larger companies
- Increased interest in consulting from companies, registrars and registries
- ISC-DLV becomes stable: Congrats.
Political interest

DNS as a political weapon

• Increased “access blocking” activities
• Most prominent model is DNS mangling
  – Answer with a “STOP” page IP
  – Shows a “STOP/Warning” page
  – Register the “visitors” for law enforcement
• ISPs deploy “dual-use” NXDOMAIN rewriting:
  – “Do you want Google to gain the money?”
DNSSEC conflicts with politics

DNSSEC detects mangling

• Common case: ISP mangling on the last mile
• Business case: Own (validating) resolver
• Advanced case: Validation after ISP resolver
  – Common to small business setups → Windows 7
  – Browser with DNSSEC plugin displays warning page: “DNS attack in process: do you want to continue?” → Will become popular.
DNSSEC Logo

Changes to former presentation

- Single registration: www.dnssec-logo.org
- Automatic (additional) data collection starts
- Requires document validation and payment
- Certificate (Image and Link) reissued monthly
- Certificate image contains zone apex and month
- History of checks available on line
DNSSEC Developments

Questions?