DNSSEC and the Zone Enumeration

Marcos Sanz
DENIC eG
sanz@denic.de

Abstract

- Known Facts
- Claimed problems
- Way ahead

Facts

- The introduction of DNSSEC with the current form of the specification provides Zone Enumeration:
  - http://josefsson.org/walker/

- An authoritative denial of existence of a given domain name **delivers** as a proof the **next existing domain name.**

- There were protocol chances to refuse AXFR

Facts

- Some key players for a successful widespread deployment of DNSSEC consider this as a **problem**:
  - Security problem?
  - Policy problem?
  - Legal problem?

Security problem?

- An attack begins by identifying your target:
  - http://www.research.att.com/~smb/papers/dnshack.pdf
- “But domain names can be gathered by other means, for instance, dictionary attacks”
  - German + English dictionary + John the Ripper = 1% of the de-zone
  - Brute force on all 8-characters delivers 13% of the de-zone.
  - com-zone as a dictionary = 42% of the nl-zone

Policy problem?

- DNS information is public...
- ...there's a **qualitative difference** between:
  - Making data available as a query/response mechanism
  - Making data available as a compilation
- DENIC's policy:

  http://www.denic.de/en/faqs/allgemeine_faqs/index.html#section_185

Legal problem?

- IANAL
- Nominet's position: http://ops.ietf.org/lists/namedroppers/namedroppers.2004/msg00687.html
- DENIC's position:
  - In conflict with Germany's Federal Data Protection Act

Way ahead

- IETF dnsext wg decided to advance the current specification as a proposed standard
- Inmediately started to work on the problem following *The Engineering Way* (TM):
  - Listing the requirements for a denial of existence
  - Weighting their relevance, since sometimes trade-offs exist
  - Evaluating proposals

Working documents

- http://www.ietf.org/internet-drafts/ draft-ietf-dnsext-signed-nonexistence-requirements-00.txt
- http://www.links.org/dnssec/requirements-matrix.htm
- http://www.links.org/dnssec/draft-laurie-dnsext-nsec2-01.txt
- http://www.ietf.org/internet-drafts/draft-arends-dnsnr-00.txt
- http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-trans-00.txt

Thanks for your attention
Any questions?