draft-ietf-dnsext-forgery-resilience

Stéphane Bortzmeyer - AFNIC

IETF 68 - Prague

Improving the integrity of DNS data, how?

DNSSEC

1. Protects the data, not only the channel
2. May be long to deploy (specially at the root)

A lightweight interim solution is welcome. To address “spoofing by guessing”.

History

"Measures for making DNS more resilient against forged answers" by A. Hubert (Netherlabs) and R. van Mook (Virtu).

1. draft-hubert-dns-anti-spoofing-00, August 14, 2006
2. Adopted by DNSEXT, January 08, 2007, with less strong language (s/MUST/SHOULD/)
3. draft-ietf-dnsext-forgery-resilience-00, January 11, 2007

A few improvements in the resolvers. . .

. . . could make things considerably safer.

Using every bit of randomness available,

The channel would be much more resilient to forgery.

The draft

1. Description of the spoofing we want to address,
2. Things the attacker has to guess or find (ID, source port, . . .),
3. Recommendations:
   - 3.1 Accept only in-zone answers,
   - 3.2 Make query parameters less guessable (with detailed calculations, see the I-D). “Add all those precious bits to the pool of bits that have to be guessed.”

Questions? Open issues?

`http://adsl-xs4all.ds9a.nl/cgi-bin/resilience.fcgi`