Making DNS answer forgery harder

ie: DNS anti spoofing

Olafur Gudmundsson for Bert Hubert
Goal: Document best practice

• Rules for implementers of DNS resolvers giving them guidance on how to:
  – Ask questions in the safest manner
  – What checks to apply to answers before accepting

• Guidance to operators to make answer forgery harder

• Document the probability of random forgery and bandwidth required.
Current State

• Status:
  – Number of implementations, comply to all or some of the recommendations
  – Number of implementations vulnerable

• Many outgoing DNS queries are from single port.
  – Multiple ports act as extending the query ID space.
WG document?

- Document is within charter
- Is document addressing a need?
- Is this approach reasonable and solid basis for compliance requirement?

- Need more people to state they support and willingness to review document.