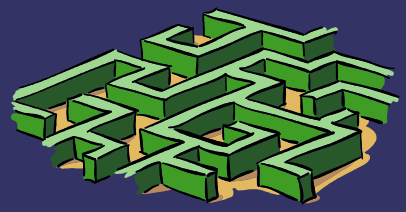
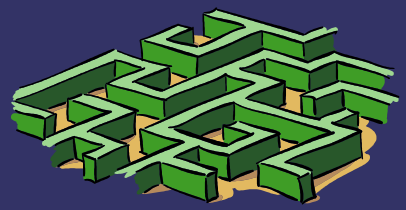
dnssec-bis-updates

Sam Weiler, Rob Austein
IETF71, Philadelphia
March 11, 2008



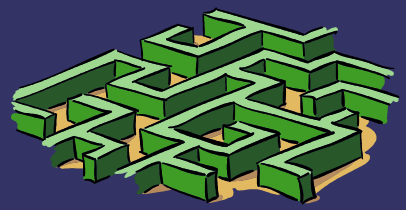
Overview

- Goals
  - Clarifications, Errata, Implementation Notes
  - And possibly minor changes?
- Open Issues
  - AD bit signaling
  - Copy CD bit to upstream queries
  - Include SOA in negative answers
- New issues?



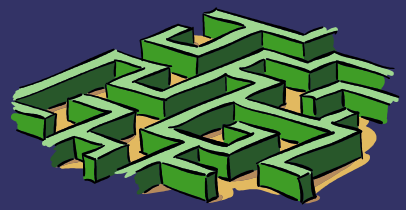
AD bit signaling

- From a discussion in September '07 on dnssec-deployment and namedroppers
- A popular implementation was setting AD even though DO was clear
- Popular DSL modems filtered these packets: signed zones not resolvable
- Proposal:
  - Have the presence of the AD bit in QUERY signal readiness to deal with AD bit in the answer
- Default action:
  - Include change, consistent w/ Sept. thread



Copy CD bit to upstream queries

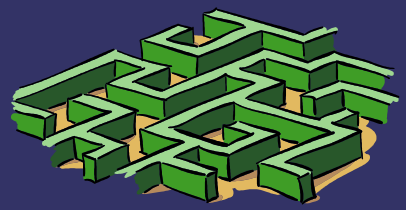
- From namedroppers, Mar '07 & Nov. '07
- Proposal:
  - "The resolver side of a security-aware recursive resolver MUST set the CD bit on its upstream queries."
- RFC4035, 3.2.2
  - “The name server side of a security-aware recursive name server MUST pass the state of the CD bit to the resolver side along with the rest of an initiating query, so that the resolver side will know whether it is required to verify the response data it returns to the name server side.”
- Default action:
  - Omit for want of discussion/support



Include SOA in negative answers

- Namedroppers, late Nov. '07
- Proposal:
  - Servers that serve DNSSEC signed zones SHOULD include SOA records in the authority section for negative answers (name error, no data). This enables clients to distinguish referrals from negative answers when the query did not set the RD bit, and validate accordingly.

    For example, a client makes a query without RD bit to its upstream caching server, and receives a reply from that cache with empty answer section, NS record present, no SOA record, no DS record in the authority section and maybe NSEC or NSEC3 records present in the authority section, and possibly A records in the additional section. The presence of the SOA record signals nodata instead of a referral. Trying to determine the message status by attempting to use (any present) NSEC records is error prone. The reason for the NSEC proof to fail may be a security failure, and using that to determine message status conflates security and message content.



New issues

- Anything else?