A path to future ways to Just say NO! in the DNS

Peter Koch
Universität Bielefeld
pk@TechFak.Uni-Bielefeld.DE

Authenticated Denial

- NSEC provides for *Authenticated Denial*
- . . . of existence (NXDOMAIN)
- . . . of content/data (NOERROR-NODATA)
- NSEC's side effect: allows full zone traversal
- Surprise!

The Task

- Identify and describe transition mechanisms
- Making an inventory of the proposed mechanisms for transition
- List the known Pros and Cons, possible security considerations
- Provide a recommendation on a way forward
  - least disruptive to DNSSEC-bis
  - keep an open path to other/new methods for auth denial

The Draft

- Team of three: Roy Arends, Jakob Schlyter, `$self`
- Short time frame (1st half of June, 2004)
- ⇝ `draft-ietf-dnsext-dnssec-trans-00.txt`

Survey (i)

- Mechanisms Updating DNSSEC-bis
  - Dynamic NSEC Synthesis (*)
  - Add Versioning/Subtyping to Current NSEC
  - Type Bit Map NSEC Indicator
  - New Apex Type
  - NSEC White Lies (*)
  - NSEC Optional via DNSSKEY Flag

Survey (ii)

- Mechanisms not Updating DNSSEC-bis
  - Partial Type-code and Signal Rollover
  - A Complete Type-code and Signal Rollover
  - Unknown Algorithm in RRSIG

Recommendation

- (Start) Work on partial TCR
- Meanwhile use NSEC synthesis

Proposed Next Steps

- Incorporate comments received so far (⇝ `-01`)
- Send `01` to WG last call
- Target: Informational RFC
- This is a just collection of ideas
  - documents wg decision and process
  - does *not* specify every method in detail
- Please read and send comments!

? – !