

# DNSSEC - an overview of recent protocol changes

March 3, 2008

bill manning - ep.net

# Some identified issues

- Zone Walking
- Resource Consumption
- Operational Training
- Cost of operation
- Lack of end system support
- ... others? ...

# Zone Walking

- DNSSEC sorts the zone data and inserts a pointer to the “next” record in the zone. The NSEC RR.
- Any successful query response will have a the next record in the zone, so a series of normal queries can enumerate the entire zone.
- Why is this a problem?

# Zone Walking - The solution

- NSEC3 - gives a “fuzzy” match on what might be next
- (nearly) impossible to guess the next record
- Voila! Enumeration of a zone through “normal” queries is foiled

# Resource Consumption

- Signing creates more and larger records
- Signing with more than one key creates more records
- The process of signing takes more compute/memory resources
- Moving signed data takes more bandwidth

# Resource consumption

- There is no single answer ...
  - Key Size
  - Number of Keys
  - Frequency and scope of Signing operations
  - Query loads
  - Number of Authoritative servers
- Several studies so far - mostly EU/US

# Operational Training

- Key Management / Escrow (big tent)
  - Managing your private keys
  - Holding keys for your children
- No longer “Fire and Forget”
- Handcrafted DNS is no longer possible
  - Tools are required

# Cost of Operation

- Hardware for crypto
- Offline/Nearline signing
- Continuity of Operations
- Emergency Key Rollover

# End System support

- Validation of the signed data occurs where?
- Still an area of active work/research
  - UNBOUND
  - BIND
  - No consistent API

# Is it worth it?

- Can DNSSEC be used to reduce registry overhead?
- UM is testing such methods now with select registrars and clients
- Using the authenticity and integrity checks from DNSSEC allow for better automation

# CADR ... so far

March 3, 2008

bill manning - ep.net

# Context

- There is a need/desire to improve or automate routine DNS activities
  - with improved authentication and integrity checks
  - timely updates
  - client driven

# What good is automation

- Reduce errors
- Reduce cost
- Client Support

**FIN**

March 3, 2008

bill manning - ep.net