Looking at TLD DNSSEC Practices

Edward Lewis, Neustar
Presented at ICANN 43, DNSSEC Workshop
March 14, 2012

neustar

Survey* Results

- As of Feb 23rd, 79 out of 302 TLDs sign (26%)
- "Most common" choices (not universal):
  - RSA SHA-1 "old guard", RSA-SHA-256 "newbies"
  - 1024 bit ZSK, 2048 bit KSK
  - One ZSK and one KSK active and present
  - NSEC3 with 1 iteration, 4 byte (8 hex char) salts, rarely/never changed
  - DS record added 3 weeks after DNSKEY appears

* *This work, thru February 1st, was presented at APRICOT 2012, the survey work continues...*

Commentary

- This work isn't exactly a "discovery" but "looking for confirmation" of previously held conventional wisdom (CW) based on workshops (1999-2004)
- Unfortunately, there were few surprises
  - Unfortunate because it means that no one is challenging the CW
- Fortunately, there were few surprises
  - Fortunate because TLDs appear to be taking a conservative approach to security

What is significant?

- TLD adoption of DNSSEC is greater than any other high-profile segment of the DNS
  - Characterized by well-developed, standards conformant DNS operations operated by capable and well equipped staff
- Are the choices made by TLDs "the way to go?"
  - Not necessarily but they are a decent suggested practice
  - Note that requirements for DNS vary by organization
  - This is a strength of the system, not a weakness

What I'd like to do

- Not "name names" when looking at operations but there are cases where "I'm curious"
  - If you operate with DNSSEC and what to see what I've observed, contact me
  - If the results are far from "norm" I'd like to know why
  - No operation that works is "wrong"

  - DNSSEC, like DNS, has no one "right way"

- My desire is to see DNSSEC work "efficiently"