Verisign DNSSEC Deployment Update

Matt Larson, VP DNS Research, Verisign Labs

22 June 2011

VERISIGN

DNSSEC Deployment Milestone Update

Zones that Verisign had a hand in signing:

- Root zone
  - Signed on July 15, 2010
- *.edu* zone
  - Signed on July 28, 2010
- *.net* zone
  - Signed on December 9, 2010
- ***.com* zone**
  - **Signed on March 31, 2011**

- A chain of trust starting at the root is now possible for well more than half of all registered domain names
  - Based on the count of domain name registrations across all TLDs from Verisign's *The Domain Name Industry Brief* (May 2011)
    - *http://www.verisigninc.com/assets/domain-name-report-may2011.pdf*

VERISIGN

DNSSEC Deployment in *.com*

- Used unvalidatable zone technique
- Timeline:
  - **February 28**: Began publishing signed zone with keys obscured
    - DNSSEC metadata returned to +DO bit queriers
    - Larger responses to +DO bit queriers
  - **March 23-24**: "Unblinded" the zone one site at a time, one server at a time
    - Methodical and cautious to ensure and verify proper DNSSEC responses from every server at every site
  - **March 31**: DS record for *.com* published in the root zone
- We received no reports of trouble
- No complaints observed in the community (mailing lists, other forums, etc.)

VERISIGN

Traffic Changes After *.com* DNSSEC Deployment

- Approximately 62% of queries have DO bit set
  - Figure has not changed substantially in years
- Bandwidth changes:
  - DNSSEC responses bandwidth: **approximately 3.75X increase**
    - Counts only responses to +DO queries
  - Overall bandwidth: **almost exactly 2X increase**
    - Counts all responses (to both +DO and -DO queries)
- TCP queries
  - Negligible increase
  - Per *.com* authoritative server: “almost none” (single digit/second) to “very few” (hundreds/second)
- Possible TCP failovers
  - UDP then TCP from same source for same <qname,qclass,qtype>
  - Another negligible increase
  - Per *.com* authoritative server: “essentially none” (<1/second) to “very few” (dozens/second)

VERISIGN

DNSSEC Uptake in *.com* (and *.net* and *.edu*)

- Registrars
  - 24 registers have at least one signed delegation (DS record) in *.net/.com* as of June 1, 2011
  - One registrar has almost 1000 signed delegations
  - A single enterprise has signed over 500 of its zones under *.com/.net*
- Signed domain name counts
  - 1,488 signed *.com* names
  - 681 signed *.net* names
  - 61 signed *.edu* names
  - See *http://scoreboard.verisignlabs.com* for up-to-date counts