Verisign DNSSEC Deployment Update

Matt Larson, VP DNS Research, Verisign Labs

NANOG 53, Philadelphia, PA

11 October 2011

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*

DNSSEC Deployment for *.com / .net / .edu*

- Resolution deployment steps (high level):
  - Slow rollout of DNSSEC-capable name server code to all DNS resolution sites
  - Publish deliberately unvalidatable zone
  - Gradual rollout of signed zone, one site at a time
  - “Unblinding” of unvalidatable zone, one site at a time
  - Add DS records to root zone
- Provisioning interface deployment steps (high level):
  - Operational Test & Evaluation (OT&E) environment for registrars
  - DNSSEC extensions enabled in live registrar-registry interface protocol
- Always allow time at each step for “baking” and issues to be discovered or reported

DNSSEC Deployment in *.com*

- Used unvalidatable zone technique
- Timeline:
  - **February 28**: Began publishing signed zone with keys obscured
    - DNSSEC metadata (e.g., digital signatures) returned to resolvers asking for DNSSEC
    - Larger responses sent to resolvers asking for DNSSEC
  - **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

Issues Encountered During Deployment

- *.edu* zone
  - None reported
- *.net* zone
  - Bug in some versions of the BIND name server affected DNSSEC validation in certain circumstances
    - Resolution failures after DS for *.net* added to root zone
    - Name servers required restart
    - Verisign reported issue to BIND developers
    - Was publicized before *.com* signing
    - Apparent low impact (one report)
- *.com* zone
  - None reported

Traffic Changes After *.com* DNSSEC Deployment

- Approximately 62% of queries request DNSSEC information
  - Figure has not changed substantially in years
- Overall bandwidth usage for responses increased almost exactly 2X
- 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 query
  - Another negligible increase
  - Per *.com* authoritative server: “essentially none” (<1/second) to “very few” (dozens/second)

DNSSEC Uptake in *.com / .net / .edu*

- Registrars
  - **36** registrars have at least one signed delegation (DS record) in *.net/.com* as of October, 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
  - **4,096** signed *.com* names
  - **1,850** signed *.net* names
  - **67** signed *.edu* names
  - See *http://scoreboard.verisignlabs.com* for up-to-date counts

Lessons Learned from DNSSEC Deployments

- **The Internet didn't break**
- Incremental deployment is possible (unvalidatable technique)
- Registrar test environment (with resolvable signed zone) helpful for every party (*.edu*)
- Monitoring is critical, especially surrounding key rollovers
- Issues with hardware and software installed base possible
  - BIND validation bug
  - Much hardware remains non-DNSSEC-capable
    - *http://verisigninc.com/assets/DataSheet-Verisign-InteropLab.pdf*

Questions?

VERISIGN™