Versign DNSSEC Update

Matt Larson, Vice President, DNS Research

ICANN 40 DNSSEC Workshop
16 March 2011
DNSSEC at Verisign: Timeline

• **.edu**
  • Zone signed and DS record published in the root zone on **July 29, 2010**
  • (Verisign operates the registry for .edu under contract with EDUCAUSE.)

• **.net**
  • Zone signed and DS record published in the root zone on **December 9, 2010**

• **.com**
  • Signed now!
  • But unvalidatable (more on that in a moment)
  • On target for DS publication in the root on **March 31, 2011**
Challenges for DNSSEC in `.com/.net/.edu`

- Sign and maintain a zone that is continually being updated
  - Tight service level agreements (SLAs) on interactions with ICANN-accredited registrars and DNS zone updates
- Safeguard cryptographic materials
- DNSSEC impact on resolution
  - Performance
  - Networking issues (fragmentation)
- Ensure valid DNSSEC responses
DNSSEC Provisioning: Architecture
DNSSEC Provisioning: New Features

• Changes to registrar interface
  • Extensible Provisioning Protocol (EPP)
  • Extended to allow DS records to be passed (RFC 5910)

• Sign changed zone data during EPP transaction

• Zone maintenance
  • Re-signing (signature refresh)
  • SOA serial number maintenance
  • Key rollover
    • KSK and ZSK
DNSSEC Provisioning: Signing and Key Mgmt

• **Signing Service**
  - Abstracts multiple HSMs (Hardware Security Module)
  - Custom signing server software, high availability (HA)

• **Key-signing Key (KSK) management**
  - Cryptographic Business Operations (CBO) group
    - Handles key material
  - “Key Signing Request” (KSR)
    - Using technique and format from root signing project
    - Communicates zone-signing keys (ZSKs) to be signed
    - Concept similar to Certificate Signing Request (CSR) in X.509
    - Response is “Signed Key Response” (SKR) containing signatures made with KSK
DNSSEC Provisioning: Need for a Signing Server

• Not practical to have an HSM for every app needing signing
  • Main servers, batch processes, admin tools, etc.
  • No HA/failover
• Need signing servers
• Benefits
  • Lower costs
  • Operational simplicity (keys, HSM management, number of components, etc.)
• Costs
  • Increased signing durations (network hops)
  • Development effort
DNSSEC Provision: HSM HA Failover
DNSSEC Provisioning: Key Management

- Collaboration with Cryptographic Business Operations (CBO) function
  - Specialize in HSMs and key management
  - Processes for security and auditing
- Provisioning of key-signing and zone-signing keys (KSKs, ZSKs)
  - KSKs kept offline
  - ZSKs loaded into HSMs and sent to provisioning data centers
- CBO pre-signs zone-apex DNSKEY data
  - Aforementioned KSR and SKR exchange
DNSSEC Parameters for .com / .net / .edu

• 2048-bit KSK
  • Lifetime of years
  • No specific plans to roll
  • Will not use RFC 5011 rollover signaling protocol

• 1024-bit ZSK
  • Rolled every three months

• Signature durations
  • DNSKEY set (made with KSK): 7 days (2-day overlap)
  • All other zone data: 7 days (4-day overlap)

• RSA/SHA-256

• NSEC3 and Opt-Out
  • For reduced zone size, not confidentiality
DNSSEC Resolution: Architecture
DNSSEC Resolution: DNSSEC validation

• Must never publish data that does not validate
  • Bad data looks like attack!
  • .com/.net/.edu can never be wrong
  • Solution: Do semantic check in addition to existing integrity checks

• Methodology
  • Verify all signatures
  • Check for NSEC3s for all published DS RRs
  • Check NSEC3 chain
  • Etc.
DNSSEC Resolution: Network

- **Fragmentation:**
  - DNSSEC responses are “large”
  - DNS works much better over UDP
  - Large UDP responses may fragment
  - Current load balancer configurations don’t work with UDP fragments

- **Fragmentation solutions:**
  - Direct Server Return (DSR)
    - Scaling issues (ironically)
    - Operational concerns
  - Just Don’t Fragment
    - Truncate DNS responses that would fragment
    - May increase DNS TCP traffic

- **Chosen solution:**
  - Just Don’t Fragment
  - DNS responses kept below Ethernet 1500-byte MTU by truncation and “truncation”
DNSSEC Deployment Approach

- Cautious and deliberate approach overall
- Deliberately unvalidatable zone
  - First used for root zone (DURZ)
  - Obscured key material to prevent validation
  - Still tests larger responses sizes and presence of DNSSEC metadata in responses

```
com. IN DNSKEY 257 3 8 (AwEAAa9Lp+THIS/IS/AN/INVALID/KEY/AND/SHOULD/NOT/BE/USED/CONTACT/INFO/AT/VERISIGN+GRS/DOT/COM+) ; key id = 30909
```
DNSSEC Deployment for .com / .net / .edu

• Resolution deployment steps (high level):
  • Slow rollout of DNSSEC-capable name server code to all 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
  • DS records added to root zone

• Provisioning interface deployment steps (high level):
  • Operational Test & Evaluation (OT&E) environment for registrars
  • EPP DNSSEC extensions enabled in live registrar interface

• Always allow time at each step for “baking” and issues to be discovered or reported
Issues Encountered During Deployment

• .edu zone
  • None reported

• .net zone
  • Bug in BIND 9.6.x and 9.7.0 affects DNSSEC validation when used as recursive name server
    • Resolution failures after DS for .net added to root zone
    • Name servers required restart
    • Have reported issue to BIND developers
    • Have publicized before .com signing
    • Apparent low impact (one report)
Lessons Learned

• The Internet didn’t break

• Incremental deployment is possible (DURZ)
• 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
Best Practices

- Deliberately unvalidatable zone and slow rollout
- Strict key management practices
- Online ZSK / offline KSK (for expediency)
- Publish DNSSEC Practice Statement (DPS)
- Validate signed data before publishing
Work with ICANN-accredited Registrars

- Software Development Kit (SDK)
- Operational Test & Evaluation (OT&E) “sandbox” environment
- DNSSEC Resource Center
- Tools guide
- Signing service
Thank You