Planning for DNSSEC

Sam Weiler
SPARTA
weiler@tislabs.com

wwTLD Community Meeting
Cape Town
30 November 2004
DNSSEC

- Allows spoofing/hijacking to be detected
  - “Did this answer really come from the zone owner?”
  - Zones are signed with public key signatures
  - Resolvers decide if they want to do validation

- Does not provide
  - Confidentiality protection (the DNS contains public data)
  - DoS protection
Why now?

• Customer/competitive pressure
  – With publication of DNSSECbis specifications and new software, your registrants will start signing their zones
• DNS's visibility as a target is increasing
  – Anti-spam records in the DNS
    • Spammers have a financial incentive to change this data
  – Growing desire to store application keys in the DNS
    • SSH keys (SSHFP)
    • IPSEC keys (opportunistic encryption)
    • Anything else where the trust model naturally aligns with the DNS heirarchy
• Better to start now, before many resolvers are doing validation
  – More time to correct mistakes
Operational Impact

• Key generation, storage

• Zone signing
  – One public-key signature per delegation
  – Repeated at a regular interval
    • Shorter interval offers children better protection
  – Can (and should) be done off-line, to protect keys

• Some zone and response size growth (~5–10x), dependent on key length
Secured Delegations: Dealing With Your Children

• Your registrants will want you to publish DS records (secure delegations) for their zones

• How to get their keys?
  – It's just another piece of data!
  – Through existing systems
  – EPP draft from Scott Hollenbeck, implemented by NeuStar
  – Direct contact registry–registrant?
Dealing With Your Parent

- If the root is signed, you will (probably) want to have a secured delegation (a DS record) in the root
  - Makes changing keys easier for you
    - You may want to encourage the signing of the root
- How do you want to send your keys to IANA?
  - Tell them!
Zone Walking

• Effectively allows zone transfers of signed zones
  – Not a (perceived) problem for many (large) registries
  – Mitigate with new WHOIS policy?
  – Do on-line signing (available now)?
  – Protocol-level solution in development, led by Nominet, ~2 years away.
    • If you need this, send requirements to namedroppers@ops.ietf.org !
Example

- VeriSign's ToDo list from KL
  - Extensions to EPP supporting DNSSEC provisioning
  - Update registry database to include DNSSEC-related information
  - Acquire cryptographic hardware
  - Define process to generate and maintain keys
  - Implement incremental signing process
  - Update zone file generation process
  - Update ATLAS (authoritative name server platform)
Resources

• Software
  – BIND 9.3.0
  – NSD 2.1.5
  – Net::DNS perl module

• Help
  – dnssec-deployment@shinkuro.com
    • Tell us what you need. Tools? Guidance?
  – www.dnssec.net
Todo

- Key generation & management
- Provisioning for signing
- DNSSEC-capable software
- How to get keys from children?
- How to send your keys to IANA?
- Send any anti-enumeration (zone-walking) requirements