Asia Pacific Network Information Centre

APNIC

APRICOT BALI 2007

APNIC DNSSEC deployment considerations

APNIC 23, Bali

George Michaelson
R&D Officer
APNIC

Overview

- DNSSEC benefits
- What we have done
- What needs to be done?
- What does APNIC need to do?
- Let's set some DNSSEC goals!

DNSSEC benefits

- Trustable DNS lookup
  - Forward and reverse
- Signed delegations
  - Positive and negative confirmations
- Some additional protections against phishing and related attacks on the DNS

What has been done

- Extensive testing of DNSSEC
  - For resolving parties
  - For domain managers
- Systems provisioning on some APNIC name servers
- Initial design discussions
  - Systems capacity planning
  - DNS management system

What needs to be done?

- Motivations: time to take a position!
- Address resolver-side issues
- Address server-side issues
- Deployment planning

Motivations

- DNSSEC standards now 10+ years in the making
  - No clear driver from APNIC community
- APNIC to research requirements and promote DNSSEC
  - Implement support in deployed servers
  - Update APNIC RMS to handle DNSSEC delegations
  - Join RIPE NCC in deploying DNSSEC in reverse-DNS

Resolver-side issues

- No date for signed root
  - Would have to distribute out of band, as RIPE NCC do
- 512 byte packet filtering considerations
  - Resolver, firewall upgrades
  - This is not only a problem for DNS
- APNIC services must work regardless of DNSSEC
  - Wish to avoid 'fate sharing' problems
    - DNSSEC outage affecting APNIC services
      - (we provision other peoples DNS)
    - Need cleaner functional separation of servers
      - Much of this already done
- APNIC no different to any DNS consumer

Server-side issues

- RIPE NCC deployment in in-addr.arpa
  - Revealed problems with APNIC secondary
    - Lack of CPU, memory
    - Software configuration issues
    - Now resolved with new hardware and software
    - Some increases in network traffic
- Key management problem
  - Managed rollovers, distribution
- No insurmountable problems
  - APNIC ready to deploy DNSSEC enabled servers in 2007 (in planning)

APNIC resource management changes

- APNIC needs a way to get “DS” info
  - The APNIC zone production process has to create a signed state over the collected DS of all sub-zones it delegates to
  - ...and generate the NSEC records to cover the ‘gaps’ in signing
- Design work needed for APNIC resource management system
  - Should aim to include DS support in 2008

Issues: shared zones

- Mechanisms for managing DNSSEC in shared zones
  - APNIC sub-zone shares with NIR
    - Solved in APNIC RMS work
  - Inter-RIR shared zones (ERX)
    - Requires inter-RIR changes
      - NRO engineering coordination group would need to coordinate

What does APNIC need to do?

- Upgrade deployed name servers
  - Done. Will be ready in 2007
- Upgrade RMS
  - DS support
  - Zone signing in DNS zone production engine
    - Requires spec work, can be ready 2008
- Progress shared zone issues
  - Discuss with key stakeholders (NIR/RIR)
    - May not be fully resolved in 2008

Lets set some DNSSEC goals!

- APNIC DNSSEC 'ready' in 2008
  - Full support in RMS, zone production
  - OOB TA distribution until root signed
- APNIC DNSSEC promoting 2007/8
  - Ongoing experiments, measurements and testing
  - Training/documentation
  - S/W & systems development
  - Active promotion of DNSSEC
    - support/assist signed root planning
- Full DNNSEC in reverse-DNS in 2008
  - Inter RIR, inter NIR. Requires coordination

Goals for 2007

- Systems deployment (already planned)
  - Server upgrades, software upgrades in progress
- NRO & NIR coordination
  - Focus on shared zone improvements
  - Plan for DS support in 2008
- Present detailed plan at APNIC 24
  - For deployment in 2008

Discussion