Agenda

- Interim Trust Anchor Repository
- Process for implementation of RZM software
- Root server “hijacking”
Interim Trust Anchor Repository
What is the ITAR?

- Interim Trust Anchor Repository
- A mechanism to publish keys of top-level domains that currently implement DNSSEC
- If the root zone is DNSSEC signed, such a repository is unnecessary
  - Therefore this is a stopgap measure
- Should be decommissioned when the root is signed
- ICANN Board voted to implement in April 2008, based on community requests
If the root was signed
It isn't so there are multiple trust apexes
Proposed registry details

- Inspired by recommendations of RIPE DNS WG
- Supports different types of DNSSEC signing
  - DS hashes either SHA-1 or SHA-256
  - DNSKEYs in any algorithm (agnostic implementation)
- Published in number of formats
  - List on website; XML structured format; Master file format
  - Should work with major software implementations
- Implementors should not be putting special ITAR provisions in code — this is meant to go away when the root is signed!
Acceptance Model

- TLD operator can submit DS key data via web form
  - DS record validated against DNSKEY data in the DNS
    - Must match before the DS key is made active in the registry.
    - DNSKEY does not need to be in the DNS at time of submission (to allow for pre-deployment), but needs to validate prior to publication.
  - Administrative and Technical contacts for the domain must consent to the listing
- Revocation is similar process, without technical test
Exit Strategy

- ITAR will be decommissioned within $x$ days of the DNS root being signed.
Limitations

- The ITAR will only operate for top-level domains
  - i.e. the keying information that would otherwise go in the root.
  - IANA will not accept anchors for descendants of top-level domains
    - Even if the relevant TLD is not signed
Why are we doing this?

- There is interest in having the DNS root zone signed with DNSSEC
- There are many unanswered questions that inhibit deployment
  - “Layer 9” issues — political, etc.
- IANA has had an operational testbed for some time signing the root zone
  - Aim is to be operationally ready once policy is set
- ITAR will assist early-adopters utilise the technology until root signing is solved
Implementation of RZM Software
Recap

- IANA is implementing “workflow automation” software
  - Supports all existing methods of root zone management
  - Also adds a new web-based management interface

- Originally driven by ccTLD community as a way to improve IANA's performance
  - IANA's performance has since improved by fixing other problems

- There are still reasons to implement the software
  - Reducing tedious manual processing, eliminate risk of re-entry errors, increased transparency in processing

- Software is based on a prototype developed by CENTR
Current issues

- To implement software changes likely will require a contract amendment
- Key personnel changes at US Department of Commerce
- New process for implementation is being developed based on new requirements from USDOC
- Working with VeriSign in developing a concrete transfer proposal to obtain approval
  - VeriSign’s scope is limited to changing the implementation phase to an internal customised EPP-based workflow
Status on testing

- Working on experimental testing with TLD operators
  - Tried testing to the various scenarios, technical tests and so forth
- Moving to parallel operations
  - Manual processing will be “primary”
  - RZM processing will be performed at same time, making sure results match
- Once comfortable of no more bugs, and relevant certification is received, flip to make RZM “primary”.
Root Server “Hijacking”
Renumbering of the L Root Server

- 198.32.0.0/16 is a block set aside for Internet Peering Points (“Exchange Points”). It was previously listed in the ARIN database as “Exchange Point Blocks”, but now to “EP.NET LLC”.

- For historical reasons, “L” root service was placed in this block amongst another allocations for peering points. (Prior to ICANN’s existence)

- As part of moving “L” out of the USC-ISI building, ICANN obtained a new net block and IP address for the service.
In liaison with the community and RSSAC, “L” was moved to the new IP address on 1 November 2007. ICANN undertook to continue service on the old IP address for a minimum of six months.

Six months later, on 2 May 2008, ICANN discontinued service.

The IP address kept responding to queries, surprising much of the Internet community.

The data being served matched that served by other root servers.
What happened?

- EP.NET LLC entered into agreement with Community DNS to provide root service on the old L root IP address.

- ICANN was not informed of this, nor were the root operators, nor the community.

- Whilst arguably within rights to delegate service in such a way, we believe it was not in the interests to take this action.
Lessons to be learnt

- There are secure routing technologies (rPKI), but they would not have helped as the IP address chain of custody was “correct”.

- Highlights issues unique to the root servers, as their old IP addresses are hard-coded in many places. Is the current IP address model for root servers correct?

- It is rather disappointing that the community was not engaged, nor was clear notice provided of the intent to continue service.

- While the net effect on end users of this event was nil, raises concerns about a bad actor doing the same thing with false data.

- More discussion at http://blog.icann.org/?p=309
Thanks!
kim.davies@icann.org