Policy Proposal 2006-3
Capturing AS Originations In Templates

Sandra Murphy
sandy@sparta.com, sandy@tislabs.com

Securing Routing Infrastructure

- Important problem, but no traction on deployable solutions
- Three workshops have been held with a wide net of the interested parties
  - Operators (ISPs, access and content providers), vendors, security geeks
  - DHS was host, anxious to find and facilitate a solution
    - See Directory Services Roundtable of ARIN XVI
    - See http://www.hsarpacyber.com/public/spri/

Operators' Emphasis

- A strong call from the operators for an ***authenticated list of authorized prefix originations***
  - Useful in responding to customer requests to route a prefix
  - Useful in debugging routing difficulties
  - Useful in building filters
  - *Necessary first step of any security for protection of BGP advertisements*

Status Last April

- Two suggestions of how to provide an authenticated list of authorized prefix originations
  - Proposal 2006-3: collect AS originations in templates
  - Resource certificate PKI panel
- Support from the audience for the idea of protecting prefix originations, mixed support for 2006-3
- AC shepherds assigned

This talk

- Readdress original proposal
- Suggest another proposal: guidance to ARIN re: goal
  - If you don’t like the specifics of 2006-3, perhaps you are willing to support the original goal 2006-3 tries to address

Formal Proposal 2006-3

- Taken from suggestion of operators in SPRI workshops:
  - Add new field in IP address resource related templates to collect ASs permitted to originate the prefix
  - Publish a collected list of authorized prefix originations without use restrictions; possibly permit individual queries as well

Exact Proposal Text

- ARIN will collect an optional field in all IPv4 and IPv6 address block transactions … used to record a list of the ASes that the user permits to originate the address prefixes …
- produce a collection of the mappings from address blocks to ASes … at least daily
- each entry will consist … of an address block, a list of AS numbers, and a tag indicating the type of delegation of the address block …
- make the collected mappings from address blocks to AS numbers available for bulk transfer …
- will not be subject to any redistribution restrictions …
- available in other forms, possibly query services …

What It Does and Doesn't Say

- What it allows
  - Requires ARIN collect originations
  - Allows ARIN to choose storage & publication
    - Could be IRR
      - AS originations used to create route object
    - Could be bulk whois
    - Could be ftp
    - Etc
  - What it does not require
    - ARIN is not attesting to origination data
      - Operator is supplying that data and is responsible for accuracy

Why ARIN?

- ARIN holds the regional authority over prefixes
- ARIN holds the regional authority over AS numbers
- ARIN is the root of all authority to speak for a prefix that is in ARIN space
  - Any structure that represented authority to speak for an ARIN prefix MUST start with ARIN
- ARIN has a ***vital, crucial role*** in constructing the authenticated list of authorized prefix originations

Why ARIN templates?

- ***Inherits operator self-discipline of completing the form and familiarity with the process***
- Inherits scrutiny of ARIN process on direct allocation/assignment
- Need ARIN to validate the authorized prefix holder anyway
- *Potential* way to populate IRR with high quality data
- *Potential* way to collect data for migration to resource certificates.

Isn’t This List Just IRR Data?

- The problem is the “authenticated” and “authorized” parts of “*an authenticated list of authorized prefix originations*”.
- Only the prefix holder speaks for the prefix
- IRRs can not authenticate a registrant as the authorized prefix holder
  - ARIN knows the authorized prefix holder (OrgID) and can authenticate POC
  - IRRs know only the mnt-by
    - That’s not always the POC
    - Even if it is, the IRR can’t authenticate the mnt-by as proper POC -- unless ARIN shares the keys
    - At last report, ARIN doesn’t validate registered route objects

Staff Comments

- *The term "user" could apply to both direct registrants as well as reassignments.*
  - Good, because that is what I meant.
- *duplicates capabilities of the routing registry and could be addressed by enhancing this existing functionality*
  - Would require synchronization of POC/mnt-by
  - Would require institution of route object validation
  - Operators are not presently registering IRR objects; they are using templates – this proposal buys into customary operational practice
  - Proposal allows ARIN to choose where to publish
- *The resource impact is significant …. Could be implemented in 3-6 months*
  - 3-6 months sounds OK to me (how many mm of effort is that?)

Some Public Comments

- Some comments said data belongs in the IRRs
  - But: *publication* was left up to ARIN anyway
    - could be IRR (create route object from template)
  - But: IRR can't do *collection* – IRRs can't authenticate registrant or validate authority
- One comment said that it would result in partial or incomplete IRR objects
  - Any IRR object created would be complete
  - Creating an IRR object would not prevent creation of others
- Some comments said the goal was the important thing (authenticated list of authorized prefix originations) – leave up to ARIN to decide how
  - This proposal suggests employing a customary operational procedure so that there is likelihood of use

Why You Might Support Goal Only: Drawbacks In ARIN Templates

- ARIN authentication of the POC is typically weak
- Using templates misses all data stored in rwhois
- The authority to originate can be expressed at allocation boundaries only
  - Given comments about the evils of de-aggregation, maybe this is a good thing :-)
- Authenticity of the collected list relies on getting it directly from ARIN; other methods (resource PKI) don’t have this limitation
- (Note: 2006-3 still good engineering start to forming the list, until/unless better assurance methods (e.g., resource PKI) become available)

Suggested Goal Oriented Proposal

- *ARIN will support and facilitate the collection and publication of an authenticated list of authorized prefix originations.*
  - A policy statement from the community to ARIN establishing a goal and priority for ARIN as part of stewardship of address resources
  - Leaves collection and publication mechanisms to ARIN
    - Could be resource PKI, could be templates, …

Can ARIN Be Responsible for Entire List?

- Some ISPs will want to take care of their own sub-allocations
  - This happens now with rwhois
  - Member choice is a good thing
  - Even so, the independent provision of sub-allocation lists has to be based ultimately on ARIN allocation/assignment – that's the "support and facilitate" part