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

Operators’ Suggestion

- New field in IP address resource related templates to collect AS’s permitted to originate the prefix
- Publish a collected list of authorized prefix originations without use restrictions; possibly individual queries as well

Proposal Text

ARIN will collect an optional field in all IPv4 and IPv6 address block transactions (allocation and assignment requests, reallocation and reassignment actions, transfer and experimental requests). This additional field will be used to record a list of the ASes that the user permits to originate address prefixes within the address block.

ARIN will produce a collection of the mappings from address blocks to ASes permitted to originate that address block, The collection will consist of a list where each entry will consist, at a minimum, of an address block, a list of AS numbers, and a tag indicating the type of delegation of the address block. This collection will be produced at least daily.

ARIN will make the collected mappings from address blocks to AS numbers available for bulk transfer in one or more formats chosen at its own discretion, informed by the community's current needs. This data will not be subject to any redistribution restrictions -- it may be republished or repackaged it any form. Should ARIN choose to use WHOIS bulk transfer as the bulk form of data access required by this paragraph, the address block to AS mappings will not be subject to any redistribution restrictions, but the remainder of the WHOIS data will remain subject to the terms of the then-current AUP regarding bulk access to WHOIS data.

ARIN may also make the collected or individual mappings from address blocks to AS numbers available in other forms, possibly query services, chosen at its own discretion, informed by the community's current needs. ARIN may require agreement to an acceptable use policy for access to the data in these forms.

Proposal Text

ARIN will **collect an optional field in all IPv4 and IPv6 address block transactions** (allocation and assignment requests, reallocation and reassignment actions, transfer and experimental requests). This additional field will be **used to record a list of the ASes that the user permits to originate address prefixes** within the address block.

ARIN will **produce a collection of the mappings from address blocks to ASes** permitted to originate that address block, The collection will consist of a list where **each entry will consist**, at a minimum**, of an address block, a list of AS numbers, and a tag indicating the type of delegation of the address block.** This collection will be produced at least daily.

Proposal Text

ARIN will **make the collected mappings from address blocks to AS numbers available for bulk transfer** in one or more formats chosen at its own discretion, informed by the community's current needs. This data **will not be subject to any redistribution restrictions** -- it may be republished or repackaged it any form. Should ARIN choose to use WHOIS bulk transfer as the bulk form of data access required by this paragraph, the address block to AS mappings will not be subject to any redistribution restrictions, but the remainder of the WHOIS data will remain subject to the terms of the then-current AUP regarding bulk access to WHOIS data.

ARIN **may also make** the collected or individual mappings from address blocks to AS numbers **available in other forms, possibly query services**, chosen at its own discretion, informed by the community's current needs. ARIN may require agreement to an acceptable use policy for access to the data in these forms.

Why ARIN?

- Inherits scrutiny of ARIN process on direct allocation/assignment
- Inherits operator self-discipline of completing the form
- Need ARIN to validate the authorized prefix holder anyway
- Potential way to populate IRR with high quality data

Why not the IRRs?

- The desired authority is: only the prefix holder is authorized to speak for the routing of the prefix
- Non-RIR IRRs can not validate the authority of the route object registerer to speak for the prefix
  - The RIR has means to authenticate the prefix holder; not necessarily a public means of authentication
- RIR IRRs can validate the authority of the route object registerer – for their own members
  - (At last report, ARIN does not do this)
  - If they allow registries from outside their membership, they are in the same boat as the non-RIR IRRs

What about the PKI Proposals?

- See *X.509 Resource and Routing Certificate* panel Monday and *An Operational ISP and RIR PKI* tutorial on Sunday re: resource PKIs
- The PKI resource hierarchy and the resource hierarchy in the ARIN whois database are the same
  - Some question as to whether they will be separate, separate but parallel, separate and unrelated, etc.
- AS capture in templates addresses the same need as the route origination attestation

Difference wrt PKI proposals?

- Surmountable difference:
  - – Authentication: PKI hierarchy is cryptographically strong; use of strong cryptography for whois is weak ☺
- Design difference:
  - – Assurance of the entries in the whois database comes from ARIN’s validation of the authentication at the time of entry; the PKI entries (certs) can be validated by anyone at any time
  - – You have to get the data from ARIN + rwhois (with a secure mechanism) to maintain original assurance in the result
  - – You do not have to get the PKI entries from the CA/ designated repository to have assurance in the result
- Implementation/Deployment/Use: easier