Using RPKI secured data for existing routing policy tools

Rüdiger Volk, Deutsche Telekom

IETF72 SIDR WG, Dublin 2008-07-28

ROA2RPSL

Executive Summary

Mapping information from ROAs to RPSL route objects with a unique source tag enables current routing policy tools to use future proof secured routing authorization information in RPKI immediately.

A quick and inexpensive way to improve routing security now, and motivation for registering routing authorization in RPKI early. RPKI is essential for later full blown secure routing protocols.

problem scenario – status quo

- need practical improvements in routing security now/ASAP; requires

  (a)authorization/authenticity in routing protocols

  (b)good information infrastructure

- without (a): emulate by policy configuration
- all networks are supposed to enforce some security policy... and would use some tools
- RPSL tools exist - but information dubious

ways to progress...

- RPKI soon provides information infrastructure
- road map for protocols unclear / how far away?
- so for interim try to make RPKI information usable for existing policy tools!
- can we map relevant RPKI information to RPSL supporting common usage models?
- yes: ROA2RPSL does the trick

What is ROA2RPSL?

- payload of **ROA**s delivers set of pairs **(prefix, ASN)**
- repositories for all globally relevant ROAs will be made available; networks may work from complete copy
- payload of RPSL **route: (prefix, ASN)**
  !!! BINGO !!! do straight direct mapping!
- map collection of *validated* ROAs to route: objects!
- unique "source:" tag defines distinct "registry" within the distributed IRR (Internet Routing Registry)
- and allows selection when querying RPSL database server

basic use of IRR data

- minimum requirement for transit provider:
  do prefix filter for customer announcements
- know your downstream customer ASs
- resolve AS set to routes registered with matching origin
  – queries may be selective and prioritize to sources
- ROA2RPSL fits in easily
- well respected IRR server can provide ROA2RPSL and make information easily available to networks that do not yet install and operate the full machinery

example ROA2RPLS route

roughly what the RIPE database server might provide

fix for Ids, URLs, official example numbers etc.

```
route6:  2007:33::/32    #ROA range 32-36
origin:  AS9.234
descr:   ROA <??whatever Id??>
descr:  <URL for repository providing ROA>
remarks: generated from a ROA in a RPKI
     <minimum disclaimer>
     for more information <URL-ROA2RPSL>
mnt-by:  RPKI-MNT
changed: roa2rpsl-demon@ripe.net 20131313
source:  ROA-IRR
```

tactics – priorities

- do NOT break existing tools
  - no syntax/semantics changes in attributes
  - be careful about additional attributes/objects
- try to feed completely unchanged tools
- use of extensions requires software development – do not depend on, but allow
- insist on exact semantics for ROA2RPSL data (exact prefix match) to avoid inconsistency when switching to “native” – i.e. secure routing protocols

few nasty details ...

- ROA can authorize a base prefix and ***many*** more specifics – can be unreasonable number to store and return with data base
- new ROA format allows to define reasonable limit (maximum length); promote reasonable use!!!
- direct mapping to standard route objects needs heuristic limit for generating standard routes
- be careful about RPSL extension to carry full information
  - comment for prefix range OK
  - additional attribute - may be possible

... and workaround

- (after sorting for origin AS) full information can be presented as standard RPSL route-sets – recommended output format for mapping tools that want to do single format: it allows
    - easy transformation to standard routes
    - some operators might adapt policy references to this kind of route-sets
- use of unrestricted ROA2RPSL information will require some small extensions/changes to existing RPSL tool chains
- allow folks doing their own tradeoff for this

example for advanced use ASENFORCEROA

- imagine: AS number 65500:65500 is reserved and declared to never be used to originate routes, name it ASENFORCEROA
- publish special semantics: ROAs that authorize this AS are indicating for the covered address space
    - ONLY routes authorized in RPKI should be accepted
    - all networks are requested/authorized to apply route filters based on ROA2RPSL enforcing origin AS

benefits of ASENFORCEROA

- helpful until RPKI has *complete* information
- filters will catch:
  - routes with unauthorized origin AS (e.g. YouTube/Pakistan Telecom)
  - unauthorized more specifics (regardless of origin)
  - bogons as far as bogon space gets registered for ASENFORCEROA

summary

- we need&want security in routing protocols
- serious improvements are needed while we wait for that
- ROA2RPSL
  - just helps as an interim solutions for that and the transition period - immediately!
  - enabling synergetic use of existing policy tools (RPSL) and the RPKI infrastructure
  - can motivate early/quick RPKI population with ROAs
- the farer the protocols are away the more ingenuity will be needed on interim solutions

minimum suggestions...

- make sure that RIRs enable support of certificates and ROAs for all applicable address space
- at least one offering complete set of ROAs mapped to a distinguished RPSL routing registry (distinct source)
- at least one free SW implementation to enable every interested network to do the mapping themselves

additional suggestions

- vendors check requirements for policy config
- promote RPKI for IPv6
  - how complete can we get filtering with ROA2RPSL?
  - could we even make better routing security a selling point for v6?
- create ASENFORCEROA and promote registration and origin validation by peers
- review/revive RPSL software to help broader use

finally...

- thanks to those who picked up the idea and are implementing or helping to push
- comments welcome
- my question: wishes of WG regarding this work?
- your questions?

so we could be close to real routing depending on RPKI

- seriously watch policy and implementation requirements of your RIR!!
- what do we operators need to do to avoid going on prime time TV news for catastrophic “failures of the Internet” due to new routing security features?
  (or only creating too much bad customer experience so customers might decide to prefer staying out of RPKI for secure routing)