

draft-spaghetti-sidrops-rpki-prefixlist

Job Snijders

Geoff Huston

The problem

- ROAs indicate an authority by the holder of a prefix for a nominated AS to originate an eBGP route for the prefix
 - A ROA does not indicate any agreement by the AS to this authority – it is a strictly “one-way” authority
- This can permit various forms of “passing off” route synthesis where a prefix holder could use a ROA in conjunction with a synthetic route to advertise a false route, and the operation of BGP would prevent the AS from directly observing this synthetic route
- An explicit “this is all I intend to advertise” construct aids in the detection and filtering of some forms of route leaks

The proposal

- It would be useful to “complete the loop” by have the AS indicate the complete set of address prefixes it may originate to any of its eBGP peers
 - Equivalent to the IRR “Route Set” construct
- This draft defines an “RPKI Prefix List”
 - It contains list of address prefixes and an AS Number, signed by the AS Number
 - It’s the maximal set of prefixes that this AS **may** originate in announcements to its routing peers

Intended use

- Any RPKI-validating BGP speaker can audit the routes that have this AS as the originating AS
- Any route originated by this AS not contained in a validated RPKI Prefix List SHOULD be regarded as invalid

Further detail

- Multiple Prefix Lists may exist concurrently
- ROA-invalid announcements that are included in an RPKI Prefix List are still invalid
- RPKI-Prefix List-invalid announcements that are in a valid ROA for this AS are still invalid

WG Adoption is requested