Verification of Routes Using Region Authorization


IETF 111
Y. Liu, ChinaMobile -- Presenter
C. Shen, CAICT
W. Yu, CAICT
H. Wang, Huawei
S. Chen, Huawei
July 23, 2021
Route Hijack Case

- Suppose AS65500 maliciously forged a more specific route originated from AS65105
- Existing hijack detection method option 1 -- RPKI ROV (RFC6810, RFC6811, RFC8210)
  - Not route origin hijack, ROV cannot detect this hijack
  - Register the ROA based on the more specific route, may cause more complex for traffic adjusting
- Existing hijack detection method option 2 -- RPKI ASPA
  - If there exists (AS65001, AS65500) (AS65104, AS65500) ASPA profiles, so ASPA cannot detect this hijack
- Either ROV or ASPA can not detect hijacks, where the way of AS-path manipulation does not violate RPKI ROA/ASPA profiles.
Proposal: Region-based Route Verification

Design Principles

- The concept of Region and Region Confederation (RC)
  - Region: consists of ASes from one ISP (e.g.,)
  - RC: consists of regions, where each region must be connected to all other regions within the RC through BGP

- Assumption
  - Routers within the same Region are trust-worthy (no hijacking)
  - Routers within the same Region Confederation are trust-worthy (no hijacking)

- Benefit
  - Protect routes, that originated within the same Region/RC, from being hijacked by non-trusted Region/RC routers

- Prerequisite of Region Verification – RPKI ROA/ROV
  - ROA/ROV provides the mapping of: routes <-- origin AS, thus provides mapping of: routes <-- origin Region/RC

- Validation rules:
  - REJECT routes, that are originated within the local Region but are received from an external region eBGP peer
  - REJECT routes, that are originated within the local Region Confederation, (not local Region) but are received from an external region confederation eBGP peer
Proposal: Region-based Verification Steps

• Step 0: region and region confederation division
  • Mutual agreement reached between cooperative ISPs

• Step 1: ISPs register their own RPKI region-based profile (to be defined):
  • ⟨RC#, region#, AS#⟩

• Step 2: routers download region-based profiles from RPKI RP server, use the region-based profiles to decide the eBGP peer roles
  • Decide if an eBGP peer (using its AS# to correlate with the region-based profile) is within the local Region or within the local region-confederation

• Step 3: routers execute ROV
  • If the prefix ROV returns “valid”, we assume that the route is originated from the origin AS in the AS-path, and thus deciding if the route is originated from the same Region/RC

• Step 4: routers execute region-based hijack validation
  • If the route is originated within local Region, but the eBGP peer is not belong to local Region, then reject
  • If the route is originated within local Region Confederation, but the eBGP peer is not belong to local Region Confederation, then reject
Application Scenario 1: Hijack Protect for routes originated within local Region

Step 1:
- ISP 1 region-based profile registration: <RC1, Region 1, AS65001>, <RC1, Region 1, AS65002>, <RC1, Region 1, AS65003>

Step 2:
- AS65001 (RC1, Region1) decides that the eBGP peers to AS65500 are not within the local region

Step 3:
- 10.2.1.1/24 received from AS65500 is valid for ROV, but it should be originated from local region

Step 4:
- Reject 10.2.1.1/24 received from AS65500, since the eBGP peer is out of region 1
Application Scenario 2: Hijack Protect for routes originated within local RC but not local Region

Step 1:
- ISP 1 region-based profile registration: <RC1, Region 1, AS65001>, <RC1, Region 1, AS65002>, <RC1, Region 1, AS65003>
- ISP 2 region-based profile registration: <RC1, Region 2, AS65104>, <RC1, Region 2, AS65105>, <RC1, Region 2, AS65106>

Step 2:
- AS65001 (RC1, Region1) decides that the eBGP peers to AS65500 (non-RC 1 member) are not belong to local RC

Step 3:
- 10.1.1.1/24 received from AS65500 is valid for ROV, but it should be originated from RC1, Region 2

Step 4:
- Reject 10.1.1.1/24 (originated from RC1, Region2) received from AS65500, since the eBGP peer from AS65500 is out of RC1
Next steps

• Need comments
Thank you!