Update on the ASPA-based AS Path Verification Draft

https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-11

K. Sriram
ksriram@nist.gov

Authors: A. Azimov, E. Bogomozov, R. Bush, K. Patel, J. Snijders, and K. Sriram

SIDROPS WG Meeting
IETF 115
November 2022

Acknowledgements: Thanks are due to many WG members in SIDROPS and GROW for comments and suggestions on the draft.

Outline of the Talk

- Changes in v-11 compared to v-09
- Comments on v-11 on the WG list
- Next steps

ASPA-based Path Verification Benefits

- Detects and mitigates BGP route leaks
- Detects and mitigates forged-origin route hijacks

Changes in v-11 compared to v-09

- Algorithm corrections per [sriram1] were made in v-09 but further refinements are made in v-11
- Additional algorithm refinements:
  - AS_SET handling
  - Route Server AS
- Other refinements
  - Clarification about applicable AFI/SAFI
  - Statement about AS Confederation
  - Overall text clarity

[sriram1] K. Sriram and J. Heitz, "On the Accuracy of Algorithms for ASPA Based Route Leak Detection, IETF SIDROPS Meeting," IETF 110 SIDROPS meeting, March 2021.
https://datatracker.ietf.org/meeting/110/materials/slides-110-sidrops-sriram-aspa-alg-accuracy-01

AS_SET Handling

- AS_SET is taken care of in the algorithm in accordance with the WG consensus
- Presence of AS_SET anywhere now makes the AS_PATH Invalid per ASPA verification algorithm
- See WG discussion and feedback about that at:

  https://mailarchive.ietf.org/arch/browse/sidrops/?gbt=1&index=02l6GBeR9E3u6ff-EB7PvoRTyds

Route Server AS

Two equivalent choices:

Choice A:

- Add the RS ASN to the AS Path in case of a transparent AS
- Apply the Algorithm for Downstream Paths

Choice B:

- Remove the RS ASN from the AS Path in case of a non-transparent AS
- Apply the Algorithm for Upstream Paths

- The draft v-11 includes Choice B
- RS-Client MUST include RS AS in its ASPA
- RS AS MUST register an AS 0 ASPA

- A figure in the backup slides provides an example showing how this works

WG discussion thread:
https://mailarchive.ietf.org/arch/browse/sidrops/?gbt=1&index=eAvyo_zOw_LfHMlY1gjJRQNqehI

Clarification about applicable AFI/SAFI

Text from v-11:

The procedures described in this document are applicable only for the address families AFI 1 (IPv4) and AFI 2 (IPv6) with SAFI 1 (unicast) in both cases [IANA-AF]. The procedures MUST NOT be applied to other address families by default.

Statement about AS Confederation

Text from v-11:

The ASes on the boundary of an AS Confederation MUST register ASPAs using the Confederation's global ASN and the procedures for ASPA-based AS path validation in this document are NOT RECOMMENDED for use on eBGP links internal to the Confederation.

Comments on Draft v-11 on the WG List

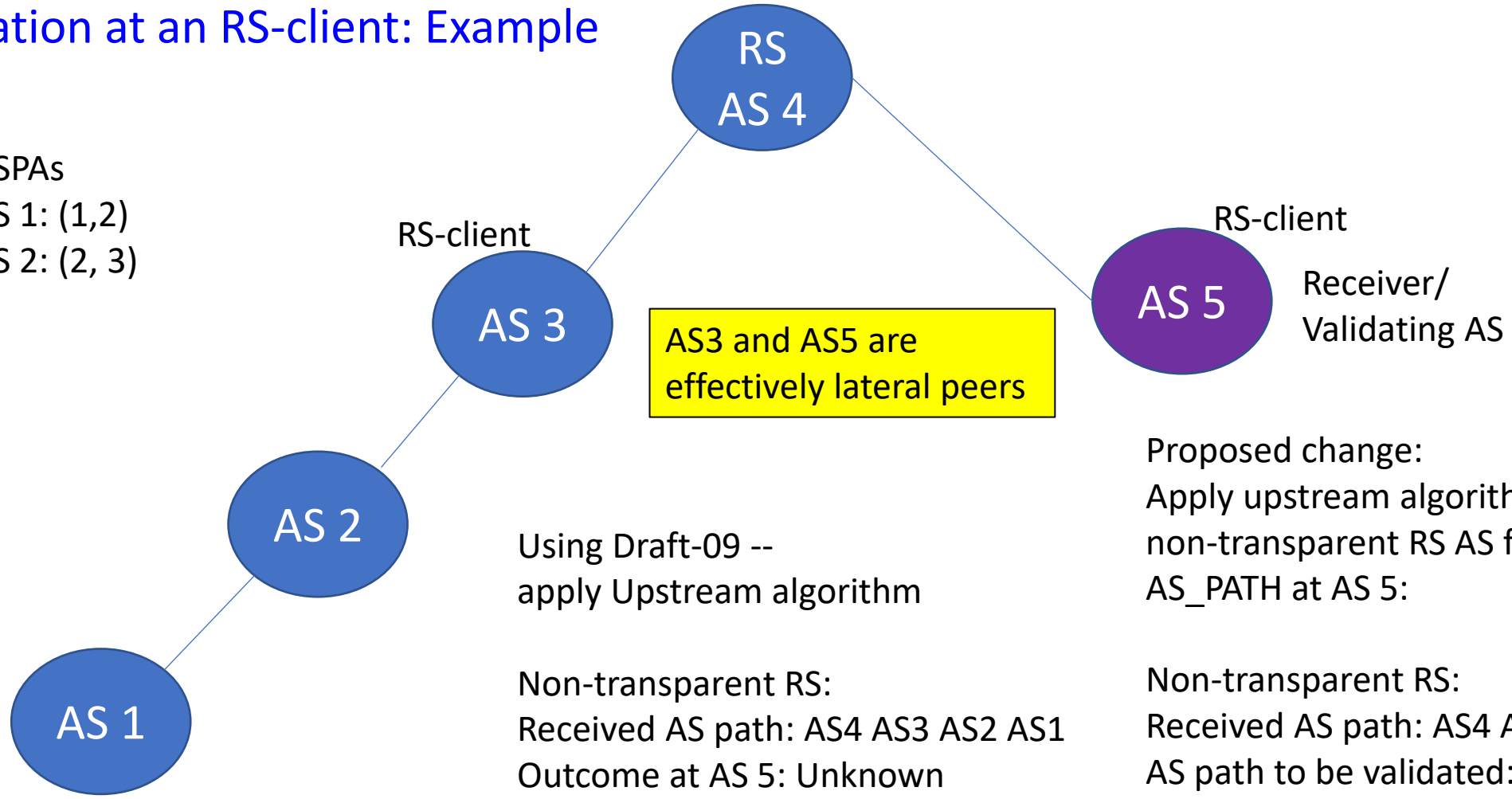
- Thanks to Claudio Jeker
- Good set of comments for improving readability
- He found [sriram1] important for understanding the draft algorithm

Next Steps

- Follow the notation and style in [sriram1] to better describe the algorithm
- Publish v-12 in the next few weeks
- Solicit implementation experience reports
- WGLC

Backup slides

Verification at an RS-client: Example



ASPAs
AS 1: (1,2)
AS 2: (2, 3)

AS3 and AS5 are effectively lateral peers

Using Draft-09 --
apply Upstream algorithm

Non-transparent RS:
Received AS path: AS4 AS3 AS2 AS1
Outcome at AS 5: Unknown

Transparent RS:
Received AS path: AS3 AS2 AS1
Outcome at AS 5: Valid

Inconsistent Outcomes

Proposed change:
Apply upstream algorithm but remove non-transparent RS AS from the AS_PATH at AS 5:

Non-transparent RS:
Received AS path: AS4 AS3 AS2 AS1
AS path to be validated: AS3 AS2 AS1
Outcome at AS 5: Valid

Transparent RS:
Received AS path: AS3 AS2 AS1
Outcome at AS 5: Valid

Consistent Outcomes

- Normally, RS-Clients will have ASPA with the RS AS included.
- Further, RS AS will have an AS 0 ASPA.