ASPA-based AS Path Verification Draft Update

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

Presenter: K. Sriram

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

SIDROPS WG Meeting
IETF 1156
March 2023

Thank you to many who participated

- Special thanks to Claudio Jeker for thorough reviews and inputs during versions 12 and 13 updates
- Many WG members participated during the WGLC and thanks to all of them

Summary

- Significant feedback and discussions during the WGLC on v-12
- Comments have been carefully considered and incorporated in version 13 (published March 28, 2023)
- Some discussion continues:
  - Single table of VAP-SPAS vs. Two (one per AFI) in the implementation
  - Verification draft procedures are described correctly
  - Implementations can structure VAP and VAP-SPAS data in whatever way they deem efficient

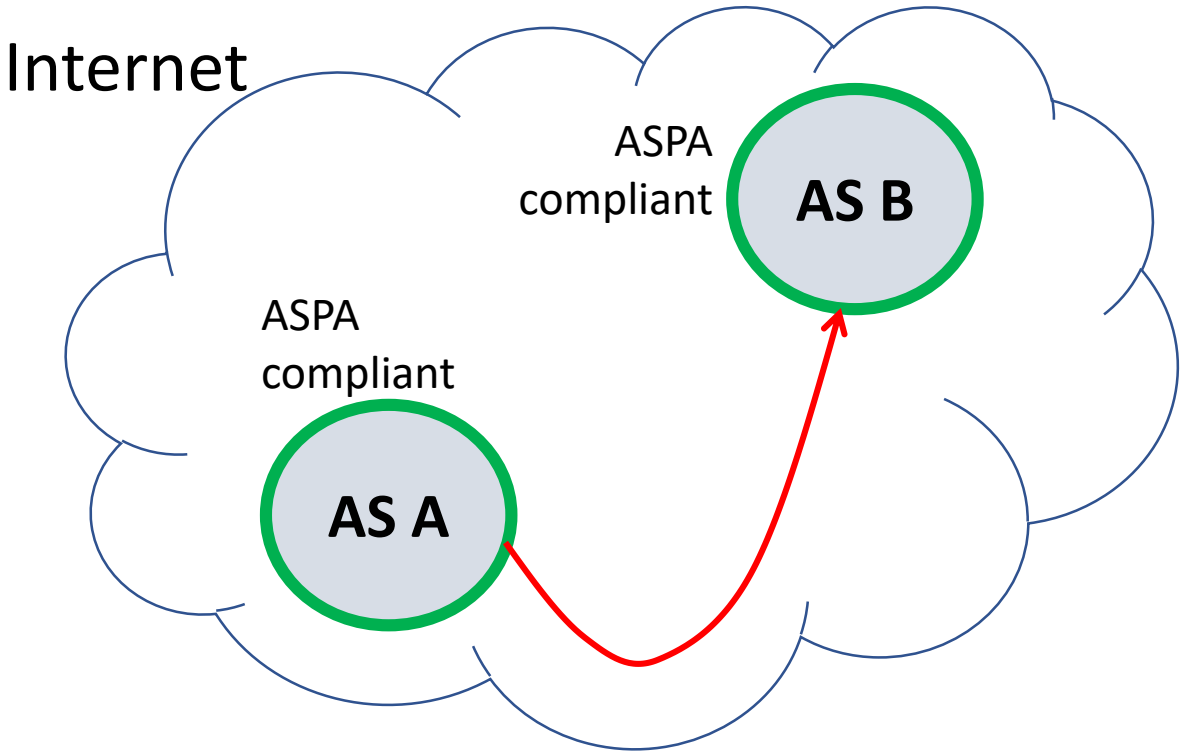
VAP = Set of Provider ASes from the Verified ASPA Payload (VAP)

Key Highlights of the Changes (v-12 to v-13)

- Sections 3, 4, and 5 refined
  - ➢ Clearer text on ASPA registration recommendations
- New explanations text on ASPA path verification properties (detection capabilities) – in Section 8

ASPA Path Verification – Properties / Detection Capabilities

ASPA Path Verification: Property 1



- AS A sends a route to a customer or lateral peer
- AS B receives the route from a customer or lateral peer
- If the AS_PATH involves a route leak…
- Always detected and mitigated at AS B

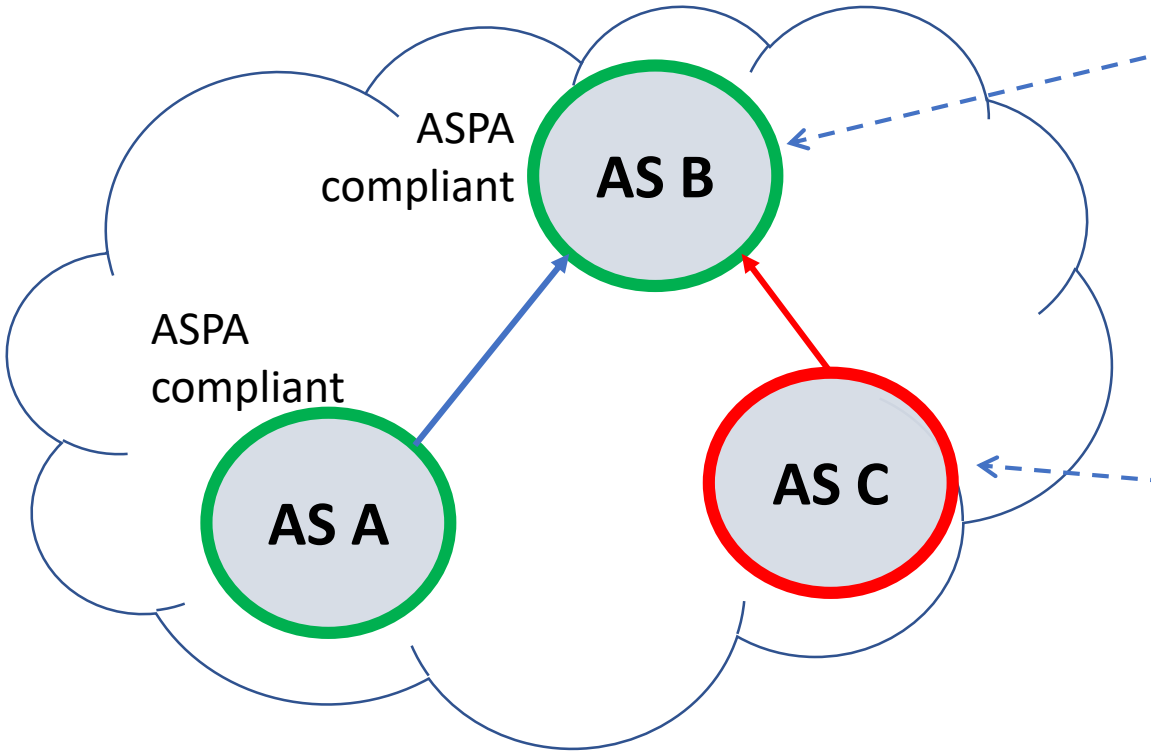
Let AS A and AS B be any two ASes in the Internet doing ASPA (generation and verification) and no assumption is made about the deployment status of other ASes. Consider a route propagated from AS A to a customer or lateral peer and leaked by an offending AS in the AS path before being received at AS B from its customer or lateral peer. The ASPA-based path verification at AS B always detects such a route leak though it may not be able to identify the AS that originated the leak. This assertion is true even when the sender AS A (or receiver AS B) is an RS AS and the neighbor AS that AS A sent to (or AS B received from) is an RS-client.

Corollary of Property 1

- In effect, if most major ISPs are compliant, the propagation of route leaks in the Internet will be severely limited.

An observation that follows from Property #1 is that if any two ISP ASes register ASPAs and implement the detection and mitigation procedures, then any route received from one of them and leaked to the other by a common customer AS (ASPA compliant or not) will be automatically detected and mitigated. In effect, if most major ISPs are compliant, the propagation of route leaks in the Internet will be severely limited.

ASPA Path Verification: Property 2

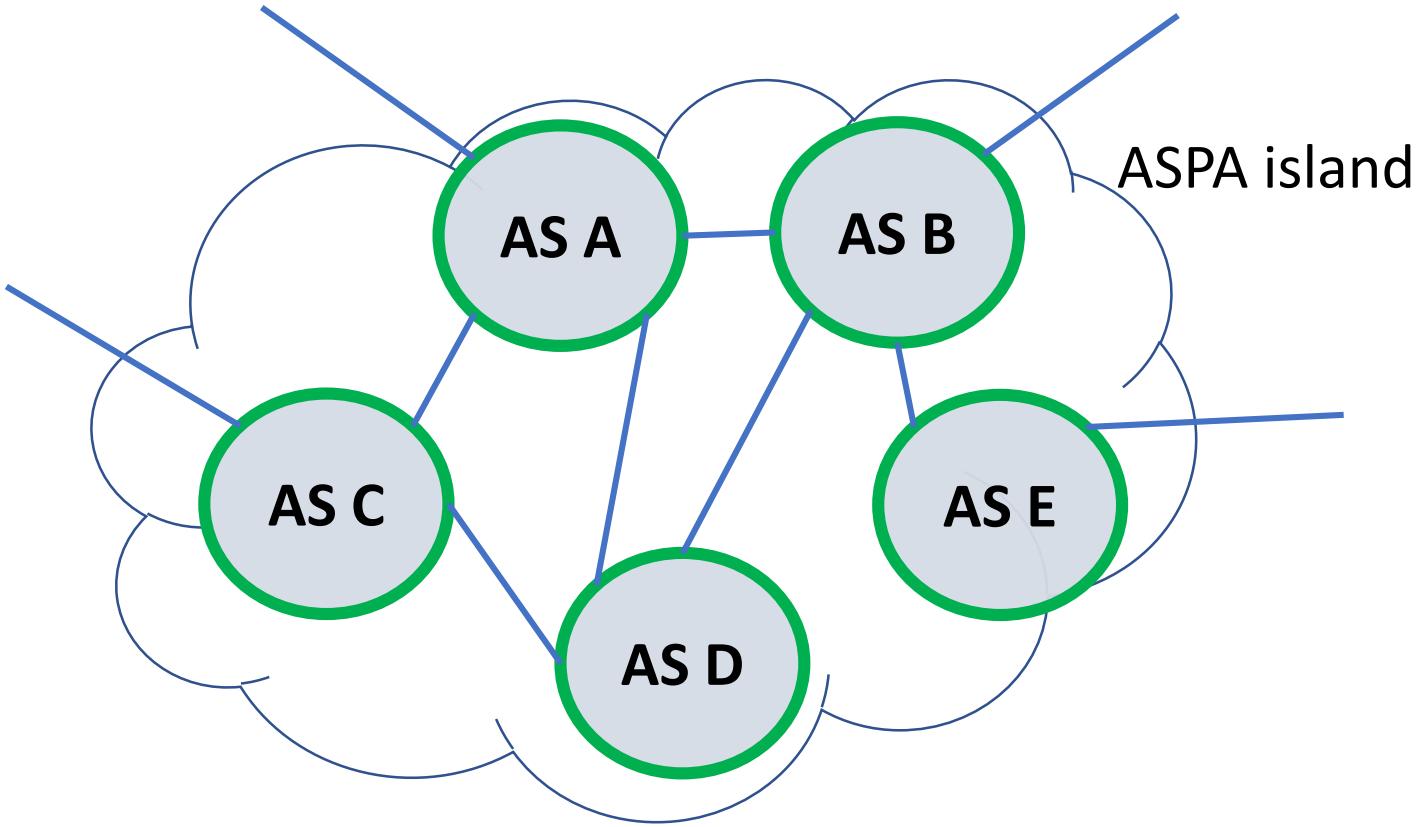


The forged-origin hijack attack is detected and mitigated at AS B

Conducts forged-origin prefix hijack involving AS A as the origin

Again let AS A and AS B be any two ASes in the Internet doing ASPA (generation and verification) and no assumption is made about the deployment status of other ASes. Consider a route received at AS B from its customer or lateral peer that is a forged-origin prefix [RFC9319] involving AS A as the forged-origin. The ASPA-based path verification at AS B always detects such a forged-origin prefix hijack.

ASPA Path Verification: Property 3

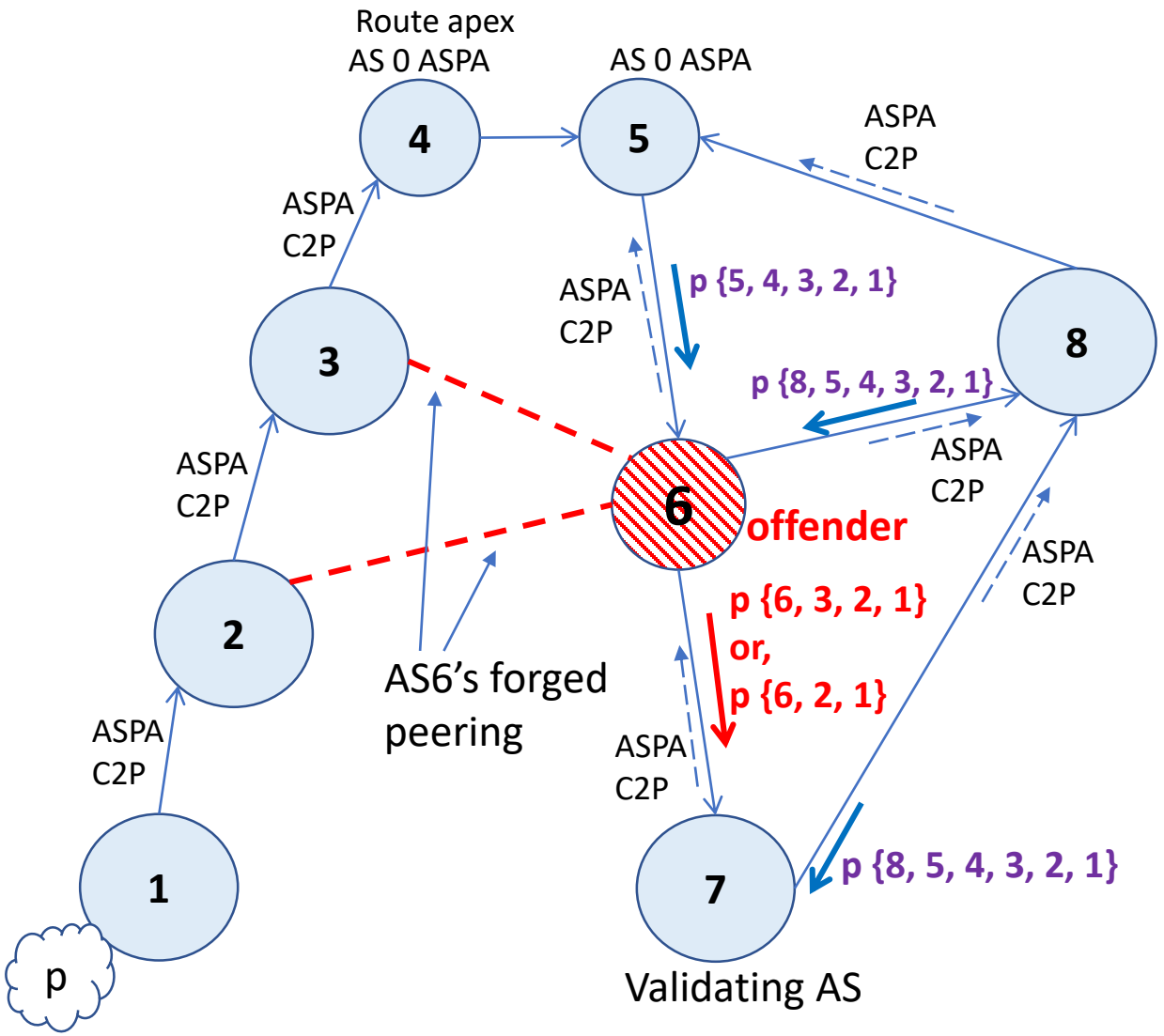


- All routes within the island are fully protected from route leaks

Consider an ASPA island (i.e., a connected set of ASPA capable ASes). Let AS A and AS B be any two ASes in the ASPA island. Consider a route propagated from AS A in any direction (i.e., to a neighbor AS with any of the BGP roles described in Section 2) and leaked by an offending AS in the AS path before being received at AS B from any direction. The ASPA-based path verification at AS B always detects such a route leak though it may not be able to identify the AS that originated the leak.

ASPA Path Verification – Short Comings

AS_PATH maliciously shortened by a provider – undetectable



C2P = Customer to Provider

- Consider AS path verification at AS 7
- All ASes are doing ASPA
- AS6 (provider) wants AS7 (customer) to prefer its path
- AS6 shortens the AS_PATH
- AS7 chooses the manipulated shorter route via AS 6

- Since other ASes are good, if AS6 does not drop customer's data traffic, then the traffic likely reaches the destination via a feasible and route-leak free path

- BGPsec can provide full AS_PATH protection
- It lacks route leak protection
- Use ASPA and BGPsec in complementary ways