

Source Address Validation in Inter-domain Networks Gap Analysis, Problem Statement, and Requirements

Dan Li, Jianping Wu, **Libin Liu**, Mingqing Huang, K. Sriram

March 17, 2025

SAVNET WG, IETF 122

Background

- ❑ This document provides a gap analysis of existing inter-domain source address validation mechanisms, describes the problem space, and defines the requirements for technical improvements.
- ❑ Historical versions
 - ◆ **draft-ietf-savnet-inter-domain-architecture-00, adopted by WG after IETF 116**
 - ◆ draft-ietf-savnet-inter-domain-architecture-01, July 24, 2023
 - ◆ draft-ietf-savnet-inter-domain-architecture-02, August 22, 2023
 - ◆ draft-ietf-savnet-inter-domain-architecture-03, February 18, 2024
 - ◆ draft-ietf-savnet-inter-domain-architecture-04, March 19, 2024
 - ◆ draft-ietf-savnet-inter-domain-architecture-05, September 9, 2024
 - ◆ **draft-ietf-savnet-inter-domain-architecture-06, December 20, 2024**
 - ◆ **draft-ietf-savnet-inter-domain-architecture-07, March 3, 2025**
 - ◆ **draft-ietf-savnet-inter-domain-architecture-08, IETF 122 SAVNET WG**

Summary of Comments and Our Responses

- ❑ Sections 4.1.3 and 4.1.4 seem to focus on the attack, rather than the spoofing. Mitigating attacks, e.g. reflection attacks, is not in the scope for the WG. (Joel)
 - ◆ **Explanation from Libin:** The scenarios described in Sections 4.1.3 and 4.1.4 are attacking, yet the root cause for the attacks is source address spoofing. Because existing solutions improperly permit the spoofing traffic, leading to severe problems.
 - ◆ **Joel's comment:** The emphasis in the text on the impact of the spoof is irrelevant and confusing. It does not matter who the false source is attacking or why. [The question SAVNET cares about is that it is spoofed traffic along a certain path. Given what you wrote, your concern is the point of insertion. So focus on that, not on distracting purpose.](#)
 - ◆ **Our response:** We have **revised the scenario description in Section 4.1** which introduces the scenario focusing on [source address spoofing traffic from a customer cone](#), and **the description in Section 4.2** which focuses on [source address spoofing traffic from a provider/peer AS](#).

Summary of Comments and Our Responses

- ❑ Section 4.1.3 seems to describe a situation that there is nothing AS 4 can do, as it cannot distinguish traffic from AS 2 that is correctly from AS 1 or from the spoofer. In this situation, AS 1 may send legitimate traffic with prefix P1 to AS 4 either directly or via AS 2. (Joel)
 - ◆ **Explanation from Libin:** The scenario (Figure 5) in Section 4.1.3 is a little different as you described. In this scenario, the forwarding path of the traffic with source addresses in P1 is AS 1->AS 4, these legitimate traffic will not reach AS 4 via AS 2. Thus, the traffic with source addresses in P1 from AS 2 is spoofing traffic.
 - ◆ **Joel' s comment:** I think you are trying to get at the case that traffic goes directly from AS1 to AS4 from P1, but not via AS2. The inclusion of the advertisement from AS 1 to AS2 with NO-Export at the very least confuses the readers. If this is indeed the scenario you are trying to cover, the text would benefit from re-writing.
 - ◆ **Our response:** We have revised the corresponding Figures to clarify the scenarios that describe existing SAV mechanisms which have improper permit problems in Section 4.1.

Summary of Comments and Our Responses

- ❑ Section 6.1.1 describes that the solution SHOULD provide improvement. It seems to me that as a requirement, **any solution MUST provide improvement at least in many cases**. If it does not, then there is no incentive to adopt. (Joel)
 - ◆ **Our Response:** We **have updated the requirement** to "It **MUST** avoid improper block and permit less spoofed traffic than existing inter-domain SAV mechanisms." in Section 6.1.1.
- ❑ Section 6.1.2 says that mechanism SHOULD NOT assume pervasive adoption. This seems to permit proposals for solutions that would require pervasive adoption. **Unless we can provide an explanation of when and why it would be acceptable to adopt a solution with such a requirement, I think we need to make this a MUST NOT**. (Joel)
 - ◆ **Our Response:** We co-authors agree with this. **Any new solutions MUST NOT assume pervasive adoption to obtain improvements**. We have revised the statement to "The new inter-domain SAV mechanism **MUST NOT** assume pervasive adoption." in Section 6.1.2.

Summary of Main Updates

- ❑ Summarize the problems of existing SAV mechanisms and technical requirements for a new SAV solution (Section 1)
- ❑ Revise the term “real forwarding paths” to “active forwarding paths” and give its definition (Section 2)
- ❑ Update the review contents of existing SAV mechanisms (Section 3)
 - ◆ Update the descriptions of ACL-based ingress filtering
 - ◆ Simplifying the contents about Virtual routing and forwarding (VRF) uRPF
 - ◆ Remove source-based remote triggered black hole (RTBH) filtering
- ❑ Update the gap analysis of existing SAV mechanisms (Section 4)
 - ◆ Remove reflection and direct attack scenarios
 - ◆ Add a scenario describing source address spoofing within a customer cone

Summary of Main Updates

- ❑ Update the gap analysis of existing SAV mechanisms (Section 4)
 - ◆ Add a scenario describing source address spoofing from a provider/peer AS
 - ◆ Remove all contents related to VRF uRPF and source-based RTBH for gap analysis
- ❑ Improve the presentation of the problem statement (Section 5)
- ❑ Improve the descriptions of the requirements for new inter-domain SAV mechanisms (Section 6)
 - ◆ Remove the comparisons for SAV using different SAV-related information individually
 - ◆ Discuss the available SAV information sources which are useful for improving validation accuracy

Updates on VRF uRPF and Source-based RTBH

□ VRF uRPF

- ◆ We focus on reviewing existing SAV mechanisms for calculating a SAV table. We co-authors discussed VRF uRPF. **VRF uRPF is not a method for computing a SAV table. It is only a way of implementation once we have got a SAV table**, for example, using strict uRPF or loose uRPF.
- ◆ Therefore, we illustrate it only in Section 3 and remove it from the gap analysis (Section 4) and problem statement (Section 5).

□ Source-based RTBH

- ◆ We also discussed this further, and think we may not see source-based RTBH as a SAV solution. SAV filtering goal is to prevent spoofing. **Source-based RTBH reacts and does damage control when DDoS attack is already happening, when the victim AS signals a specific prefix or IP address to the neighbor AS.**
- ◆ This draft discusses SAV mechanisms documented by RFCs and thus should not include source-based RTBH.

SAV-related Information Sources

- SAV-related information sources

- ◆ Local routing information
- ◆ RPKI ROA and ASPA objects
- ◆ SAV-specific information

- This document recommends the [above SAV-related information sources](#) which are useful for improving validation accuracy, instead of comparing the SAV table results using them for SAV individually

Problem Summary of Existing Mechanisms

❑ Problems of existing SAV mechanisms

- ◆ **Improper block:** Existing uRPF-based mechanisms suffer from improper block in two inter-domain scenarios: limited propagation of prefixes and hidden prefixes.
- ◆ **Improper permit:** Existing uRPF-based mechanisms exhibit improper permit in scenarios involving source address spoofing within a customer cone or from a provider/peer AS.
- ◆ **High operational overhead:** ACL-based ingress SAV filtering introduces significant operational overhead, as it needs to update ACL rules manually to adapt to prefix or routing changes in a timely manner.

Requirements for a New SAV Solution

- ❑ To address the above problems, this document outlines the following technical requirements for a new solution
 - ◆ **Improving validation accuracy over existing mechanisms:** A new solution **MUST** avoid improper block and minimize improper permit.
 - ◆ **Reducing operational overhead:** A new solution **MUST** have less operational overhead than ACL-based ingress SAV filtering.
 - ◆ **Working in incremental/partial deployment:** A new solution **MUST NOT** assume pervasive adoption and **SHOULD** provide effective protection for source addresses when it is partially deployed in the Internet.
 - ◆ **Providing necessary security guarantee:** A new solution **SHOULD** secure the communicated information between ASes if it requires exchanging specific information between ASes.
 - ◆ **Guaranteeing convergence:** A new solution **SHOULD** achieve accurate SAV rule convergence in response to prefix or routing changes.

Requirements for a New SAV Solution

- ❑ To address the above problems, this document outlines the following technical requirements for a new solution
 - ◆ **Improving validation accuracy over existing mechanisms:** A new solution **MUST** avoid improper block and minimize improper permit.

We have consolidated these points in the Introduction Section to facilitate readers' rapid comprehension of the document's key points.

pervasive adoption and **SHOULD** provide effective protection for source addresses when it is partially deployed in the Internet.

- ◆ **Providing necessary security guarantee:** A new solution **SHOULD** secure the communicated information between ASes if it requires exchanging specific information between ASes.
- ◆ **Guaranteeing convergence:** A new solution **SHOULD** achieve accurate SAV rule convergence in response to prefix or routing changes.

Acknowledgements

- Many thanks to Jared Mauch, Barry Greene, Fang Gao, Anthony Somerset, Yuanyuan Zhang, Igor Lubashev, Alvaro Retana, Joel Halpern, Aijun Wang, Michael Richardson, Li Chen, Gert Doering, Mingxing Liu, John O'Brien, Roland Dobbins, etc. for their valuable comments on this document.

Next Step

- Request WG Last Call

Thanks! 😊