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

Dan Li, Jianping Wu, **Lancheng Qin**, Mingqing Huang, Nan Geng

July, 2025

Background

- This informational document includes
  - A **gap analysis** of the current operational intra-domain SAV mechanisms
  - **Informational requirements** for technical improvements that should be considered when designing the future intra-domain SAV architecture and solution
- Document history
  - draft-li-savnet-intra-domain-problem-statement-00, Jul 2022
  - draft-ietf-savnet-intra-domain-problem-statement-00, May 2023
  - **WGLC, Aug. 23--Sep. 6, 2024**
  - **IETF Last Call, Jan. 3--Apr. 3, 2025**
  - **Returned to the SAVNET WG, Apr. 3, 2025**

Background

- Main concerns
  - ◆Standards-track protocol changes must be based on standards-track requirements
    - ➢But the current requirements are informational
  - ◆Some terms are not clearly defined
- Suggestions from our responsible AD
  - ◆**Share** the latest version **with the impacted WGs (e.g., LSR)** to get broader input
  - ◆Split the document into two parts
    - ➢An informational document that outlines the use cases and identifies technology gaps
      - ✓Remain the current informational requirements and make it clear that these requirements cannot be used to initiate protocol changes
    - ➢A standards-track document that clearly defines the normative requirements for protocol solutions

Background

- Share with the LSR WG (May 19, 2025 & Jun. 06, 2025)

- Request this presentation to help LSR participants become familiar with the document and its background

- Clarification
  - ◆**No IGP extensions are currently foreseen**
  - ◆This document **does not describe any solution design or protocol requirements**
  - ◆Any protocol changes would require a standards-track requirements document, not a non-normative reference to this informational document

Terminology

- Sub Network
  - A sub network may operate its own internal routing protocols (e.g., a separate IGP), but it is considered part of the AS in the global routing system. It is connected to one or more routers of the AS for Internet connectivity. It originates traffic but does not transit traffic for other networks.
- Improper Block
  - The validation results that the packets with legitimate source addresses are blocked improperly due to inaccurate SAV rules
- Improper Permit
  - The validation results that the packets with spoofed source addresses are permitted improperly due to inaccurate SAV rules

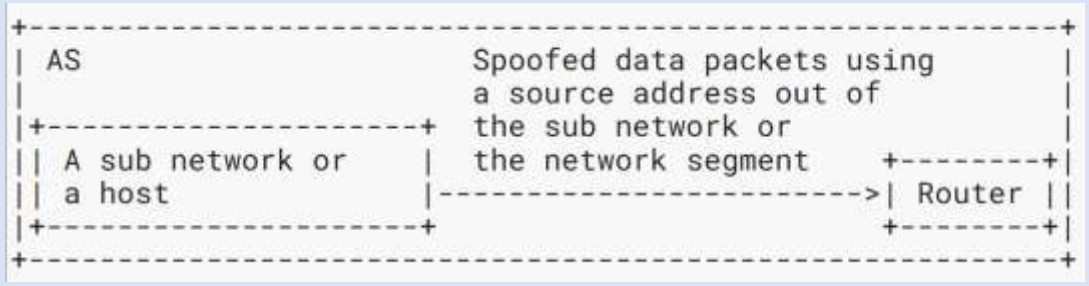
Boundary between Intra-domain SAV and Inter-domain SAV

- Intra-domain SAV
  - Intra-domain SAV for an AS determines SAV rules by the AS itself with its own information (e.g., local configuration or intra-domain routing information)
- Inter-domain SAV
  - Inter-domain SAV for an AS requires information (e.g., Border Gateway Protocol (BGP) data) provided by other ASes to determine SAV rules

Use Cases of Intra-domain SAV

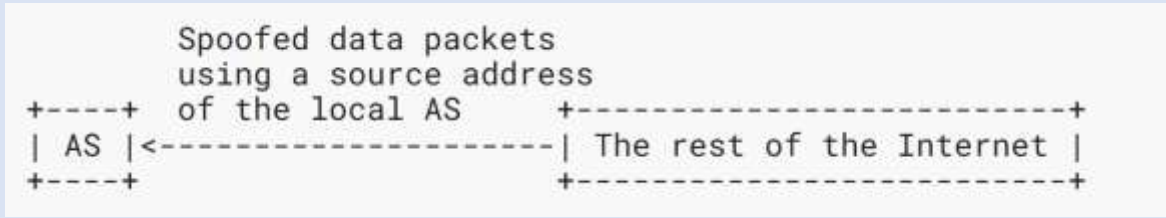
Use Case #1: Intra-domain SAV for traffic originating from sub networks or hosts within the AS

Prevent a sub network from using a source address out of the sub network or prevent a host from using a source address out of the network segment



Use Case #2: Intra-domain SAV for traffic sent from the rest of the Internet

Prevent spoofed data packets coming from the rest of the Internet that use a source address of the local AS



Current Operational Intra-domain SAV Mechanisms

- Access Control List (ACL) [RFC2827, BCP38]
  - A SAV filter that checks the source address of every data packet against a list of acceptable or unacceptable prefixes. The ACL rule is typically configured and updated manually
- Strict uRPF [RFC3704, BCP84]
  - It implements a SAV filter in an automatic way. It accepts a data packet only when i) the local FIB contains a prefix covering the packet's source address and ii) the corresponding outgoing interface for the prefix in the FIB matches the packet's incoming interface
- Loose uRPF [RFC3704, BCP84]
  - It also uses the local FIB to implement SAV but checks only for the existence of the prefix. It can be used to block spoofed data packets using a non-global or non-routed source address

Problem Statement

- ACL-based SAV
  - Problem: **High operational overhead**
  - Reason: Entirely relying on manual maintenance
- Strict uRPF
  - Problem: **Improper block** under **asymmetric routing** and **hidden prefix** scenario
  - Reason: Solely using the router's local FIB information to determine SAV rules, which may not match the incoming interfaces of legitimate data packets from the source
- Loose uRPF
  - Problem: **Improper permit**
  - Reason: Allowing any spoofed data packet using a source address covered by the FIB

General Requirements

- Accurate Validation
  - MUST improve the accuracy upon existing intra-domain SAV mechanisms
- Automatic Update
  - MUST automatically generate and update SAV rules on, rather than relying entirely on manual updates
- Working in Incremental Deployment
  - MUST specify the deployment scope and provide incremental benefits when incrementally deployed within the specified deployment scope
- Fast Convergence
  - MUST update SAV rules in time when prefix changes, route changes, or topology changes
- Security
  - MUST NOT introduce additional security vulnerabilities or confusion to the existing intra-domain architectures or protocols

Thanks!