Charter for SAVNET Working Group

Source address validation (SAV) is one important way to mitigate source address spoofing attacks. Therefore, it is desirable to deploy SAV in intra-domain and inter-domain networks. However, existing SAV mechanisms like uRPF-related technologies may improperly permit spoofed traffic or block legitimate traffic.

The "Source Address Validation in Intra-domain and Inter-domain Networks (SAVNET)" working group will define protocol-independent architectures and procedures whose accuracy improves upon current SAV mechanisms. Specifically, the SAVNET WG will define mechanisms to accurately determine valid incoming physical or virtual router interfaces for specific source prefixes.

The scope of the SAVNET WG includes the SAV function for both intra-domain and inter-domain networks and the validation of both IPv4 and IPv6 addresses. The WG will address intra-domain solutions first. SAVNET should avoid packet modification in the data plane. Existing control and management plane protocols should be used within existing architectures to implement the SAV function. Any modification of or extension to existing architectures or control or management plane protocols must be carried out in the working groups responsible for them and in coordination with this working group.

The SAVNET WG is chartered for the following list of items:

(1) Problem Statement, Use Cases, and Requirements

This document should include an analysis of the current solutions and their limitations. This item may require one document to address intra-domain SAV and another to address inter-domain SAV.

(2) SAVNET Architecture Documents

This item requires one document to address intra-domain SAV and another to address inter-domain SAV. Each document must describe the conditions under which the architecture can improve accuracy or performance with respect to existing SAV mechanisms without assuming pervasive adoption. Each document must also include a threat model of the proposed architecture and a comparison to existing SAV mechanisms.

(3) Definition of protocol-independent operation and management mechanisms to operate and manage SAV-related configurations.

After each of the items above has reached WG consensus, a discussion about whether it is appropriate to continue must occur. The discussion can consider topics related to the accuracy of the mechanism and the types of attacks it can prevent. The WG Chairs will define the

specific criteria and determine that rough consensus has been reached before continuing. The WG may be rechartered or closed if rough consensus is not reached.

The SAVNET WG will coordinate and collaborate with other WGs as needed. Specific interactions may include (but are not limited to):

* lsr for OSPFv2, OSPFv3 and IS-IS extensions
* idr for BGP extensions
* lsvr for BGP SPF extensions
* rift for RIFT extensions

Each of these other WGs can independently determine the applicability and priority of SAV to their deployments.

Milestones:

Nov 2022: Adopt the Problem Statement, Use Cases, and Requirements document

Jul 2023: Submit the Problem Statement, Use Cases, and Requirements document to the IESG for publication

Jul 2023: Adopt the Intra-Domain Architecture document

Mar 2024: Submit the Intra-Domain Architecture document to the IESG for publication

Mar 2024: Adopt operations and management for Intra-domain networks document

Mar 2024: Adopt the Inter-Domain Architecture document

Jul 2024: Submit operations and management for Intra-domain networks document to the IESG for publication

Nov 2024: Submit the Inter-Domain Architecture document to the IESG for publication

Nov 2024: Adopt operations and management for Inter-domain networks document

Mar 2025: Submit operations and management for Inter-domain networks document to the IESG for publication