Inter-domain Source Address Validation (SAVNET) Architecture

Jianping Wu, Dan Li, Mingqing Huang, Li Chen,

Nan Geng, **Libin Liu**, Lancheng Qin

November 8, 2023

Outline

- Background
- Review of Requirements for the New Inter-domain SAV Mechanism
- Main Updates Compared to Version 03
- Inter-domain SAVNET Architecture
- Summary

Background

- Inter-domain SAVNET architecture aims to provide a comprehensive framework for developing new inter-domain SAV mechanisms
  - Address the problems of existing inter-domain SAV mechanisms
  - Meet the requirements proposed in [draft-ietf-savnet-inter-domain-problem-statement]
- Historical versions
  - draft-wu-savnet-inter-domain-architecture-00, IETF 115 SAVNET WG
  - **draft-wu-savnet-inter-domain-architecture-01, IETF 116 SAVNET WG**
  - draft-wu-savnet-inter-domain-architecture-02, June 1, 2023
  - **draft-wu-savnet-inter-domain-architecture-03, IETF 117 SAVNET WG**
  - draft-wu-savnet-inter-domain-architecture-04, September 30, 2023
  - **draft-wu-savnet-inter-domain-architecture-05, IETF 118 SAVNET WG**

Comments on Version-03

- Rüdiger Volk: whether or when a basic model of SAV-specific message content is introduced?
  - Response: In Section 2, we have illustrated the content of SAV-specific message, which is used to communicate source prefixes and their legitimate incoming interfaces, and in Section 6.1, we have illustrated it in detail with an example.
- Ben Maddison & K. Sriram: SAV-specific protocol should not be used to distribute information for forwarding.
  - Response: It does not communicate forwarding information between ASes. We have revised Section 6.1 to illustrate that a SAV-specific information communication mechanism is needed to communicate source prefixes and their legitimate incoming interfaces between ASes.

Comments on Version-03

- Jeffrey Haas: should discuss what incremental means in deployment considerations.
  - Response: In Section 8, we have discussed what incremental deployment is, why incremental deployment is needed to support, and how inter-domain SAVNET can support it in the partial/incremental deployment considerations.
- Jeffrey Haas: should add the considerations for the convergence and scalability.
  - Response: We have added Section 9 to discuss the convergence considerations, which discuss that inter-domain SAVNET should guarantee convergence and propose suggestions about how to avoid improper blocks and reduce improper permits during the convergence process. Also, inter-domain SAVNET should have high scalability to support Internet-level SAV.

Comments on Version-03

- Joel Halpern: need to distinguish between incremental deployment of support for the SAV protocol and its information incremental deployment of acting on the SAV information.
  - Response: In Section 8, we have distinguished the partial/incremental deployments of inter-domain SAVNET architecture and SAV information sources.
- K. Sriram: You will include the forwarding path in the SAV-specific message. Does it contain an AS path?
  - Response: The SAV-specific message does not contain the AS path of BGP NLRI announcements. In Sections 2 and 6.1, we have illustrated the SAV-specific information, which contains the source prefixes and their legitimate incoming interfaces to enter other ASes.

Comments on Version-03

- Alvaro Retana: What type of information is the SAV-specific information? The "forwarding path information" seems to indicate the routing or forwarding information, rather than SAV information. If existing routing protocol is used to transmit the SAV information, it is needed to note that existing routing mechanism cannot be affected.
  - Response: In Section 6.1, we have illustrated the contents of SAV-specific information, which are different from the traditional routing or forwarding information. Also, we have illustrated how inter-domain SAVNET can obtain the SAV-specific information and communicate it between ASes. A SAV-specific information communication mechanism may be needed to communicate the SAV-specific messages between ASes, and if it is implemented by extending existing protocol, the protocol should not be affected.

Comments on Version-03

- Igor Lubashev: The section differentiates between "SAV-specific Information" (information developed exclusively for SAV) and "General Information" (other information). It does not anticipate "dual-use" information -- information developed for both SAV and non-SAV purposes. While "SAV-specific Information" would, indeed, require a new protocol to disseminate, the "dual use" information may be disseminated using an existing protocol.
  - Response: In Section 5, we have added the discussion on SAV-specific information, general information, and dual-use information. Indeed, the general information defined in the draft represents the information for both SAV and non-SAV purposes, and can also be called dual-use information.

Comments on Version-03

- Igor Lubashev: It is valuable to make a distinction between Static "General Information" (such as information from registries or manual configs) and Dynamic "General Information" (such as information from RIB). Dynamic is the only kind of information that can be used to discover the real forwarding paths, because real forwarding paths can change at any time. It should be noted that depending on the implementation, a change of a real forwarding path may be reflected in the SIB with a delay. Therefore, it is more robust to use Static General Information for discovering permissible paths, especially for inter-domain solutions.
  - Response: In Sections 5 and 9, we have made a distinction and added these considerations into the convergence considerations and suggested to use the stable general information during the convergence process of the SAV-specific information.

Outline

- Background
- Review of Requirements for the New Inter-domain SAV Mechanism
- Main Updates Compared to Version 03
- Inter-domain SAVNET Architecture
- Summary

Review of Requirements for the New Inter-domain SAV Mechanism

- Requirement #1: Improving Validation Accuracy over Existing Mechanisms
- Requirement #2: Working in Incremental/Partial Deployment
- Requirement #3: **Guaranteeing Convergence**
- Requirement #4: Reducing Operational Overhead
- Requirement #5: Communicating SAV-specific Information between ASes
- Requirement #6: **Securing the Communicated SAV-specific Information**

Outline

- Background
- Review of Requirements for the New Inter-domain SAV Mechanism
- **Main Updates Compared to Version 03**
- Inter-domain SAVNET Architecture
- Summary

Main Updates Compared to Version 03

- Revise the Design Goals section
- Revise the SAV Information Base section
  - Refine the definition of SAV-specific information and general information
  - Add the illustration for priority rankings of different SAV information sources
  - Revise the examples in Figures 3 and 4 and their relative descriptions
- Add a new SAVNET Communication Channel section
- Add a new Use Cases section
- Revise the Partial/Incremental Deployment section
- Revise the Convergence Considerations section
- Revise the Security Considerations section

Outline

- Background
- Review of Requirements for the New Inter-domain SAV Mechanism
- Main Updates Compared to Version 03
- **Inter-domain SAVNET Architecture**
- Summary

Key Idea of Inter-domain SAVNET Architecture

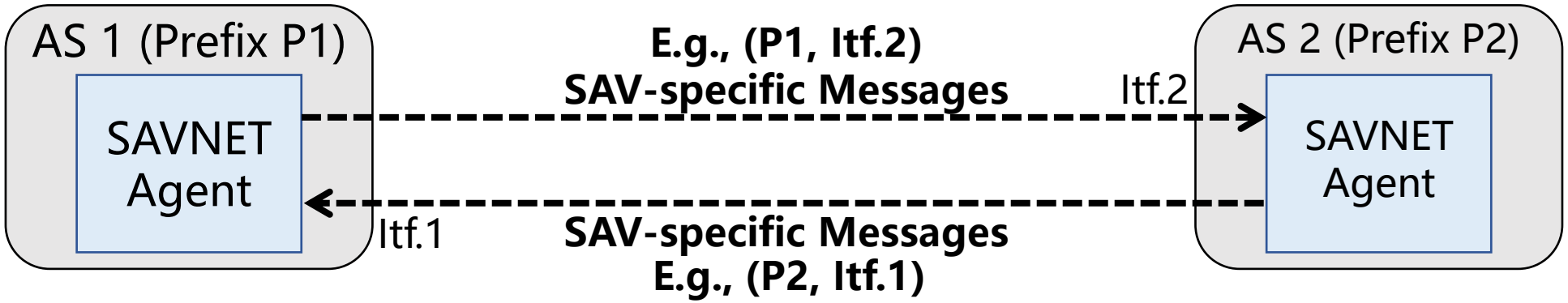
- Generating SAV rules with SAV-specific information
  - When SAV-specific information is available, SAV-specific information is preferentially used to generate SAV rules
    - SAV-specific information is specifically designed to generate more accurate SAV rules than the information used in existing inter-domain SAV mechanisms, e.g., local routing information
  - A new SAV-specific information communication mechanism would be developed to deliver the SAV-specific information
    - The SAV-specific information communication mechanism should deal with the route changes carefully to avoid false positives
- When the SAV-specific information is unavailable during the stage of partial/incremental deployment, inter-domain SAVNET will generate SAV rules with the general information

SAV-specific Information and General Information

- SAV-specific information is the information designed specifically for SAV and consists of source prefixes and their corresponding incoming interfaces
- General information refers to the information that is not originally designed for SAV but can be used for SAV to some extent
  - Such as the relationships between prefixes and ASNs in RPKI ROA objects, the Customer-to-Provider relationships in RPKI ASPA objects, and the local routing information in RIBs or FIBs
  - Compared to dynamic general information, e.g., information from the RIB, stable general information, e.g., information from RPKI, is more authoritative and can generate more accurate SAV rules to help avoid improper blocks, especially for the convergence process

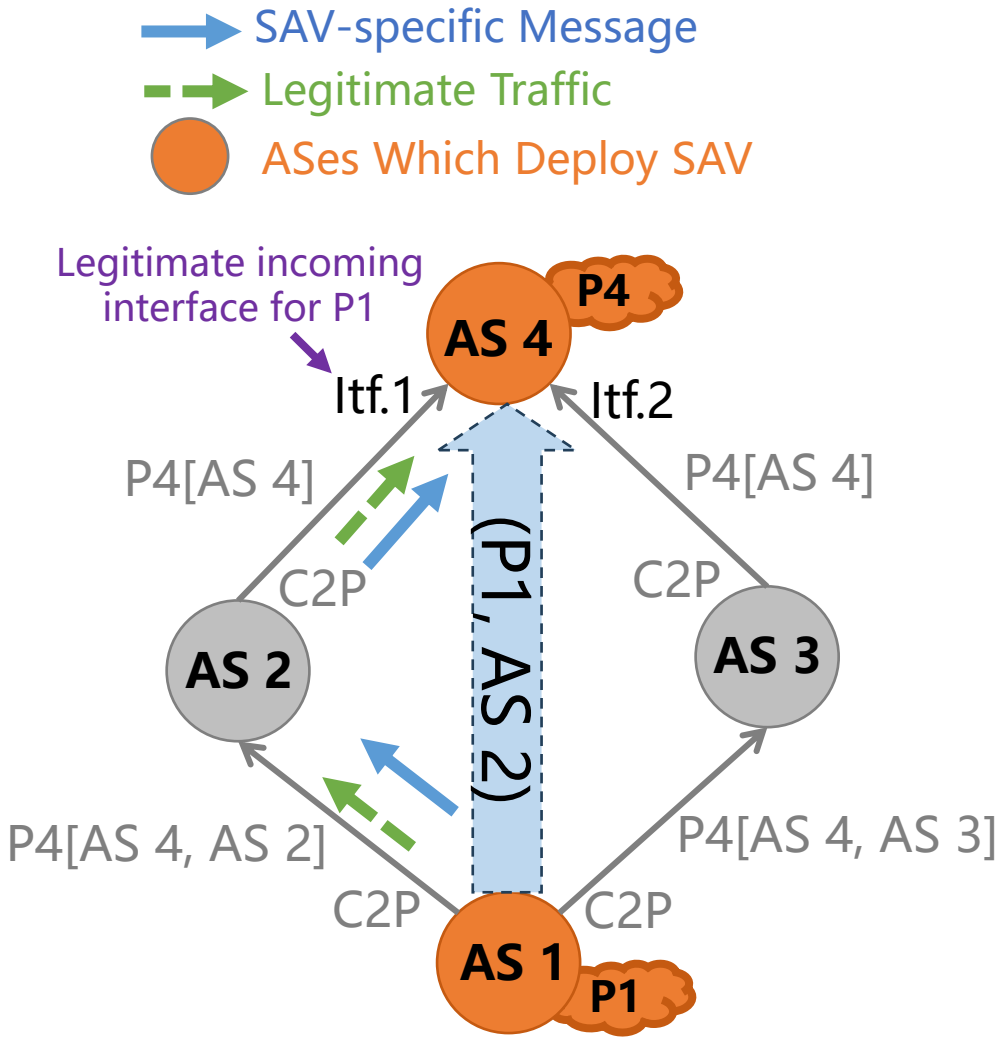
SAV-specific Information Communication Mechanism

- The SAV-specific information communication mechanism define how the SAV-specific messages are used to communicate the SAV-specific information between the SAVNET agents in different ASes
  - For an AS which originates the SAV-specific messages, its SAVNET agent puts its own source prefixes and the corresponding incoming interfaces in the SAV-specific messages by checking its local RIB and sends them to the corresponding ASes which perform SAV
  - For an AS which receives SAV-specific messages from other ASes, its SAVNET agent can parse the SAV-specific messages and obtain the legitimate incoming interfaces for the source prefixes of the origin AS



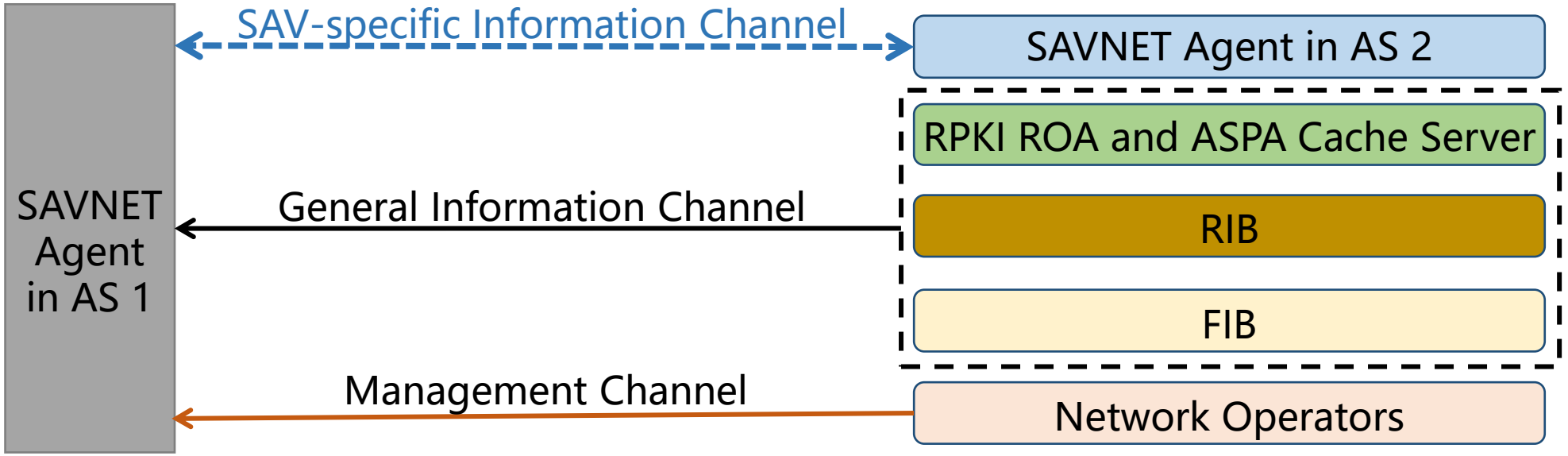
An Example for Illustrating SAV-specific Information Communication Mechanism

- Assume the paths of all legitimate traffic from AS 1 to AS4 are AS 1→AS 2→AS 4
- By using the SAV-specific information communication mechanism, AS 1 advertises its source prefix and the corresponding incoming interface, e.g., (P1, AS 2), with the SAV-specific message along the path AS 1→AS 2→AS 4
- After parsing the SAV-specific message originated from AS 1, AS 4 obtains that the legitimate traffic with AS 1' s source prefix P1 as source addresses will come from AS 2 and arrive at the interface Itf.1.



SAVNET Communication Channel

- SAV-specific Information Channel
  - The abstraction of the connections for communicating SAV-specific information
- General Information Channel
  - The abstraction of the connections for obtaining general information
- Management Channel
  - The abstraction of the connections for obtaining manual configurations, such as YANG, CLI, SAVNET operation and management, and inter-domain SAVNET provisioning



Partial/Incremental Deployment Considerations

- Inter-domain SAVNET should support partial or incremental deployment
  - The partial/incremental deployment of the inter-domain SAVNET architecture consists of the partial/incremental deployment of the architecture and the partial/incremental deployment of the SAV information sources
  - A SAVNET agent should easily form a logical connection with the SAVNET agent deployed in other ASes. This connection can be established through manual configurations or an automatic neighbor discovery mechanism
  - When the SAV-specific information for some prefixes are unavailable, the general information (e.g., routing information from the RIB or FIB) should be used to generate SAV rules for these prefixes
- To reduce the deployment risks, network operators can enable the block action incrementally
  - Sampling→rate limiting→blocking

Convergence Considerations

- SAVNET agent should collect the SAV-specific information and the general information and consolidate them in a timely manner
  - For the SAV-specific information, the SAVNET agent should launch SAV-specific messages to adapt to route changes in a timely manner
  - For the general information (e.g., routing information, ROA objects, or ASPA objects), it relies on the convergence mechanisms in routing protocols or RPKI
- SAV-specific information communication mechanism should be designed with consideration of factors that may affect the convergence
  - Such as packet loss, unpredictable network latency, or message processing latency
- Stable general information, such as information from RPKI ROA and ASPA objects, can be used to generate SAV rules during the convergence process of the SAV-specific information

Security Considerations

- The security threats faced by the SAV-specific information communication mechanism in inter-domain networks can be categorized into two main aspects:
  - Session security threats
    - Session identity impersonation and session integrity destruction
  - Content security threats
    - Message alteration, message injection, and path deviation
- Existing security mechanisms (e.g., MD5, Keychain) can be used or a new security mechanism should be designed to secure the SAV-specific information
  - The detailed security design of the SAV-specific information communication mechanism is out of scope for this document

Outline

- Background
- Review of Requirements for the New Inter-domain SAV Mechanism
- Main Updates Compared to Version 03
- Inter-domain SAVNET Architecture
- Summary

Summary

Inter-domain SAVNET can meet the requirements proposed in [draft-ieft-savnet-inter-domain-problem-statement]

- Requirement #1: Improving Validation Accuracy over Existing Mechanisms
  - SAV-specific information can generate more accurate SAV rules than general information
- Requirement #2: Working in Incremental/Partial Deployment
  - When some SAV-specific information is not available, general information can still be used
- Requirement #3: Guaranteeing Convergence
  - The SAVNET agent should launch SAV-specific messages to adapt to route changes in a timely manner
- Requirement #4: Reducing Operational Overhead
  - SAV information can be automatically collected through SAVNET communication channels
- Requirement #5: Communicating SAV-specific Information between ASes
  - SAV-specific information communication mechanism is designed to make it
- Requirement #6: Securing the Communicated SAV-specific Information
  - Existing security mechanisms can be used or a new security mechanism can be designed

Acknowledgements

- Many thanks to Alvaro Retana, Kotikalapudi Sriram, Rüdiger Volk, Xueyan Song, Ben Maddison, Jared Mauch, Joel Halpern, Aijun Wang, Jeffrey Haas, Xiangqing Chang, Changwang Lin, Mingxing Liu, Zhen Tan, Yuanyuan Zhang, Yangyang Wang, etc. for their valuable comments and feedback on this document.

Thanks! ☺