Inter-domain Source Address Validation (SAVNET) Architecture

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

March 19, 2024
SAVNET WG, IETF 119
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
  - draft-wu-savnet-inter-domain-architecture-06, February 5, 2024
  - draft-wu-savnet-inter-domain-architecture-07, IETF 119 SAVNET WG
Improving the presentation of the inter-domain SAVNET architecture

- **Add a new architecture figure** displaying the network topology and the communication flow of the SAV-related information (Joel & Aijun)
- Suggest that the draft adds data plane considerations (Xueyan)
- Suggest that the draft draws multiple links between two neighbouring ASes in the figures including network topology, and clearly states which SAV (AS level or link level) the inter-domain SAVNET architecture performs (Joel)
- Suggest that the draft adds a paragraph that clearly states how the inter-domain SAVNET architecture provides the incentive (Joel)

Adding more considerations about SAV information sources

- We can use IRR data to automatically update ACL rules. The problem is that IRR data is not validated (Antoin)
- How you can trust the ASes which send you information (Antoin & Aijun)

Clarifying the descriptions of some concepts

- No need of SAV-specific communication channel (Huaimo)
- Clarify that SAV-specific information is more accurate, timely, and trustworthy than other information (Joel)
Response #1: We Have Improved the Presentation of the Inter-domain SAVNET Architecture

- In **Section 1**, we have added a new paragraph to illustrate the incentive of inter-domain SAVNET architecture.

- In **Section 4**, we have added a new architecture figure, displaying the AS-level topology and the communication flows of all the SAV-related information, and added high-level descriptions about the SAV data plane.

- In **Sections 4 and 8**, in all figures, we have added multiple links for neighboring ASes to indicate that inter-domain SAVNET performs AS-level SAV, and we have also explained this in **Section 4**.

We have discussed these updates in the mailing list.
Response #2: We Have Added More Considerations about the SAV Information Sources

- In **Section 5.1**, we have added a new section to discuss IRR data and included it in the general information for inter-domain SAV. Additionally, both Paul Vixie (SIE Europe) and Michael Richardson (Sandelman) have discussed the concerns about the availability, accuracy, and slow update of the IRR data.

- In **Section 7.1**, we have added the requirement that SAVNET agent should validate the authenticity of the connection for communicating the SAV-specific information to verify whether the SAV-specific information is provided over a secure connection with an authenticated AS.

We have discussed automatic ACL rule updates using IRR data and the validation requirement of SAV-specific information in the mailing list.
Response #3: We Have Clarified the Concepts of Information Channels and SAV-related Information

- In Section 1, we have summarized the accuracy, timeliness, and trustworthiness of SAV-specific information. We have added a new Section 5 to illustrate all the SAV-related information and distinguished them in terms of SAV accuracy, timeliness, and trustworthiness.

- In Section 7.1, we have removed SAV-specific information channel and described the SAV-specific information communication mechanism, which can be implemented by extending an existing protocol or a new protocol.

We have discussed the SAV-specific information and the SAV-specific information communication mechanism in the mailing list.
Main Updates Compared to Version 05

- Revise the Introduction Section
  - Summarize SAV-specific information and general information and their differences
  - Explain the incentive of the inter-domain SAVNET architecture
  - Summarize the accuracy, timeliness, and trustworthiness of SAV-specific information

- Revise the Design Goals Section
  - Remove the descriptions for a communication mechanism for SAV-specific information and move this to Section 7.1

- Revise the Inter-domain SAVNET Architecture Overview Section
  - Add a new inter-domain SAVNET architecture figure
  - Add the relative contents to overview the architecture and the SAV-related information and illustrate that inter-domain SAVNET performs AS-level SAV
  - Add the high-level data plane considerations

- Add a new SAV-related Information Section

- Revise SAV Information Base Section

- Revise SAVNET Communication Mechanism Section

- Revise Use Cases Section
Main Updates Compared to Version 05

- Revise the Introduction Section
  - Summarize SAV-specific information and general information and their differences
  - Explain the incentive of the inter-domain SAVNET architecture
  - Summarize the accuracy, timeliness, and trustworthiness of SAV-specific information

- Revise the Design Goals Section
  - Remove the description for a communication mechanism for SAV-specific information

- Add the relative contents to overview the architecture and the SAV-related information and illustrate that inter-domain SAVNET performs AS-level SAV
- Add the high-level data plane considerations

- Add a new SAV-related Information Section
- Revise SAV Information Base Section
- Revise SAVNET Communication Mechanism Section
- Revise Use Cases Section

All the updates have been discussed and illustrated in the mailing list of SAVNET WG.
Inter-domain SAVNET Architecture Overview

- **AS X’s Provider AS**
- **AS X’s Lateral Peer AS**
- **AS X’s Customer AS**

- **AS-level topology**
- **Communication flow of the SAV-related information**
  - **SAV-specific information**
    - AS X and one of its customer ASes have deployed SAVNET agent and can exchange SAV-specific information with each other.
  - **RPKI ROA object and ASPA object**
  - **Local routing information**
  - **IRR Data**

- **AS-level inter-domain SAV**

**Diagram Elements:**
- IRD Database
- RPKI Cache Server
- BGP Message
- SAV-specific Message
- IRR Data
SAV-related Information

<table>
<thead>
<tr>
<th>SAV-related Information</th>
<th>SAV Accuracy</th>
<th>Timeliness</th>
<th>Trustworthiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRR Data</td>
<td>Improper Block &amp; Improper Permit</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Local Routing Information</td>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RPKI ROA Obj. &amp; ASPA Obj.</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SAV-specific Information</td>
<td>Functioning as Expected</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- **General Information**
  - IRR data: IRR data **may not be accurate and are updated in a slow manner**.
  - Local routing information: SAV based on local routing information **may lead to improper blocks or improper permits in many scenarios** as analyzed in [draft-ietf-savnet-inter-domain-problem-statement].
  - RPKI ROA objects and ASPA objects: In some partial deployment scenarios, they may **lead to improper blocks or improper permits**. They are stable but not updated in a timely manner, and thus may lead to improper blocks when prefixes or routes change.

- **SAV-specific Information**
  - SAV-specific information includes prefixes and their incoming directions for accurate SAV, and can **be updated automatically in a timely manner**, and SAVNET agent validates the authenticity of the connections for communicating SAV-specific information.
SAV Information Base

Data structure of SAV information base (SIB)

- SAVNET agent uses SIB to consolidate SAV-related information.
- Each row records the index, the prefix, the prefix’s valid AS-level incoming direction, the AS relationship, and the corresponding information source.

<table>
<thead>
<tr>
<th>Index</th>
<th>Prefix</th>
<th>Incoming Direction</th>
<th>Relation</th>
<th>SAV Information Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>P1</td>
<td>AS 2</td>
<td>Customer</td>
<td>SAV-specific Information</td>
</tr>
<tr>
<td>1</td>
<td>P1</td>
<td>AS 1</td>
<td>Customer</td>
<td>General Information</td>
</tr>
<tr>
<td>2</td>
<td>P2</td>
<td>AS 2</td>
<td>Customer</td>
<td>General Information</td>
</tr>
<tr>
<td>3</td>
<td>P3</td>
<td>AS 3</td>
<td>Provider</td>
<td>General Information</td>
</tr>
<tr>
<td>4</td>
<td>P5</td>
<td>AS 3</td>
<td>Provider</td>
<td>General Information</td>
</tr>
<tr>
<td>5</td>
<td>P5</td>
<td>AS 5</td>
<td>Customer</td>
<td>General Information</td>
</tr>
<tr>
<td>6</td>
<td>P6</td>
<td>AS 2</td>
<td>Customer</td>
<td>General Information</td>
</tr>
<tr>
<td>7</td>
<td>P6</td>
<td>AS 1</td>
<td>Customer</td>
<td>SAV-specific Information</td>
</tr>
</tbody>
</table>
How to Utilize the SAV-related Information in the SIB to Generate Accurate SAV Rules

- Using priorities of different SAV information sources
  - Inter-domain SAVNET architecture assigns priorities to different SAV information sources and preferentially uses information source with higher priority to generate SAV rules

<table>
<thead>
<tr>
<th>Priority Ranking for the SAV Information Sources</th>
<th>SAV Information Base for AS 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAV Information Sources</td>
<td>Priorities</td>
</tr>
<tr>
<td>SAV-specific Information</td>
<td>1</td>
</tr>
<tr>
<td>General Information</td>
<td></td>
</tr>
<tr>
<td>ROA and ASPA Obj.</td>
<td>2</td>
</tr>
<tr>
<td>RIB</td>
<td>3</td>
</tr>
<tr>
<td>FIB</td>
<td>4</td>
</tr>
<tr>
<td>IRR Data</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SAVNET Communication Mechanisms

- **SAV-specific information communication mechanism**
  - SAV-specific information communication mechanism is used for communicating SAV-specific information and it can be implemented by extending an existing protocol or a new protocol.

- **General information communication mechanism**

- **Management mechanism**
The Incentive of Inter-domain SAVNET Architecture

In the scenario where AS 1 does not deploy the inter-domain SAVNET architecture, existing uRPF-based SAV mechanisms would block the legitimate traffic with SA in P1 and DA in P4 improperly.

If both AS 1 and AS 4 have deployed the inter-domain SAVNET architecture, AS 1 can communicate the SAV-specific information to AS 4, AS 4 will be aware of that the traffic with P1 as SA can arrive at the interface facing AS 2, and thus forward it properly.
Summary

- New inter-domain SAV mechanisms developed following the inter-domain SAVNET architecture can meet the requirements proposed in [draft-ieft-savnet-inter-domain-problem-statement].

- The inter-domain SAVNET architecture and its updates have been presented during the meetings of IETF 115, 116, 117, and 118, and this document addresses all the comments from our community and is discussed in the mailing list of SAVNET WG.

  ♦ draft-wu-savnet-inter-domain-architecture-07, IETF 119 SAVNET
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, Antoin Verschuren etc. for their valuable comments and feedback on this document.
Next Step

- Call for WG adoption
Thanks! 😊
Key Idea of Inter-domain SAVNET Architecture

- Generating SAV rules with SAV-specific information
  - When **SAV-specific information is available, it is preferentially used** to generate SAV rules
    - SAV-specific information is **specifically designed to generate more accurate SAV rules** than the information (e.g., local routing information) used in existing inter-domain SAV mechanisms
  - A new SAV-specific information communication mechanism would be developed to carry the SAV-specific information
    - The SAV-specific information communication mechanism should deal with the route changes carefully to avoid **false positives**

- When SAV-specific information is unavailable during its partial/incremental deployment, generating SAV rules with general information
SAV-specific Information and General Information

- **SAV-specific information** is the information designed specifically for SAV and consists of their legitimate 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, and the Customer-to-Provider relationships in RPKI ASPA Objects, local routing information in RIBs or FIBs, and IRR data.
  - Compared to dynamic general information, such as information from 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 what information the SAV-specific messages carry and how they communicate

SAV-specific information between the SAVNET agents in different ASes

- For an AS which originates SAV-specific messages, its SAVNET agent puts its own source prefixes in the SAV-specific messages and sends them to all the potential destination ASes by checking the local RIB

- For an AS which receives SAV-specific messages from other ASes, its SAVNET agent can obtain the legitimate incoming directions for the source prefixes of the origin AS
Assume the paths of all traffic from AS 1 to AS 4 are AS 1→AS 2→AS 4.

By using the SAV-specific information communication mechanism, AS 1 advertises its own source prefixes with SAV-specific messages along the path AS 1→AS 2→AS 4.

After receiving the SAV-specific message originated from AS 1, AS 4 identifies the legitimate incoming direction for source prefix P1 of AS 1, i.e., (P1, AS 2), and terminates the message.