Inter-domain Source Address Validation (SAVNET) Architecture

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

Mar 29, 2023
Introduction

- Inter-domain SAV is important for mitigating source address spoofing attacks
  - Preventing traffic that forges other ASes' source addresses from entering the AS that deploys inter-domain SAV

- However, existing inter-domain SAV mechanisms have limitations
  - uRPF-related SAV mechanisms have improper block or improper permit problems
  - ACL-based SAV mechanisms have high operational overhead problems

- To address the limitations,
  - Inter-domain source address validation (SAVNET) architecture provides a framework for developing new SAV mechanisms
Design Goals

Inter-domain SAVNET architecture aims to enhance accuracy and facilitate partial deployment with low operational overhead

- **Accurate SAV at peer and customer interfaces**
  - Accurately learn the valid source addresses that should be **permitted** and block packets with the learned invalid or other unknown source addresses

- **Accurate SAV at provider interfaces**
  - Accurately learn the invalid source addresses that should be **blocked** and permit packets with the learned valid or other unknown source addresses

- **Automatic update**
  - Adapt to dynamic networks and asymmetric routing scenarios automatically

- **Working in partial deployment**
  - Provide protection for the source prefixes of deployed ASes in partial deployment scenario
Scope

Different from Version-00 which focuses on the specific new SAV mechanism, Version-01 focuses on **high-level architecture**

- This draft focuses on
  - High-level architecture designs that enable an AS to generate accurate SAV rules by using SAV-related information from various sources

- This draft does not include
  - Protocol designs or protocol extensions
  - Detailed solutions for reducing operational overhead, since they should be considered in specific SAV mechanisms
  - Detailed solutions for collecting and updating SAV-related information from different sources
Inter-domain SAVNET Architecture

- Basic idea
  - Consolidate SAV-related information from multiple sources and generate SAV rules based on the SAV-related information

- Main components
  - SAV-related information sources
  - SAV Information Manager (SIM)
  - SAV Information Base (SIB)
  - SAV table
Inter-domain SAVNET Architecture

- **Basic idea**
  - Consolidate SAV-related information from multiple sources and generate SAV rules based on the SAV-related information

- **Main components**
  - SAV-related information sources
  - SAV Information Manager (SIM)
  - SAV Information Base (SIB)
  - SAV table
SAV-related Information Sources

- SAV-related information that specifies the valid incoming interfaces for a source prefix can be learned from
  - Manual Configuration
    - SAV-related configurations from YANG, command-line interface (CLI), and protocols such as remote triggered black hole (RTBH) and Flowspec
  - Passive Acquired Information
    - Topological and routing information from Routing Information Base (RIB), Routing Information Messages, RPKI ROA objects, and RPKI ASPA objects
  - Active Collaboration Information
    - Real forwarding paths of prefixes transmitted by Collaborative Messages from other ASes

- All sources are optional depending on the availability of them and operational needs
Inter-domain SAVNET Architecture

- Basic idea
  - Consolidate SAV-related information from multiple sources and generate SAV rules based on the SAV-related information

- Main components
  - SAV-related information sources
  - SAV Information Manager (SIM)
  - SAV Information Base (SIB)
  - SAV table
SAV Information Manager (SIM)

- **Function #1**
  - Maintain the Source Information Base (SIB) by consolidating SAV-related information collected from multiple sources

- **Function #2**
  - Generate SAV rules to fill out the SAV table in data plane based on the SIB
Inter-domain SAVNET Architecture

- **Basic idea**
  - Consolidate SAV-related information from multiple sources and generate SAV rules based on the SAV-related information

- **Main components**
  - SAV-related information sources
  - SAV Information Manager (SIM)
  - SAV Information Base (SIB)
  - SAV table
SAV Information Base (SIB)

- **Data structure of SIB**
  - Each row records the index, the prefix, the prefix’s valid incoming interface, the prefix’s incoming direction, and the corresponding information source
  - Different information sources may specify different incoming interfaces for the same prefix

### SAV Information Base for AS X

<table>
<thead>
<tr>
<th>Index</th>
<th>Prefix</th>
<th>AS-level Interface</th>
<th>Direction</th>
<th>Information Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>P1</td>
<td>Itf.1</td>
<td>Provider</td>
<td>Collaborative Message, Routing Information Message</td>
</tr>
<tr>
<td>1</td>
<td>P1</td>
<td>Itf.2</td>
<td>Provider</td>
<td>Routing Information Message, RIB</td>
</tr>
<tr>
<td>2</td>
<td>P2</td>
<td>Itf.2</td>
<td>Provider</td>
<td>Manual Configuration</td>
</tr>
<tr>
<td>3</td>
<td>P3</td>
<td>Itf.3</td>
<td>Peer</td>
<td>Collaborative Message, RPKI ROA objects, RPKI ASPA objects</td>
</tr>
<tr>
<td>4</td>
<td>P4</td>
<td>Itf.4</td>
<td>Customer</td>
<td>Collaborative Message</td>
</tr>
<tr>
<td>5</td>
<td>P4</td>
<td>Itf.5</td>
<td>Customer</td>
<td>Routing Information Message, RIB</td>
</tr>
<tr>
<td>6</td>
<td>P5</td>
<td>Itf.5</td>
<td>Customer</td>
<td>Routing Information Message, RIB</td>
</tr>
</tbody>
</table>
SAV Information Base (SIB)

- Data structure of SIB
  - Each row records the index, the prefix, the prefix’s valid incoming interface, the prefix’s incoming direction, and the corresponding information source
  - Different information sources may specify different incoming interfaces for the same prefix

- How to identify the most accurate incoming interfaces from multiple information sources?
  - Finer-grained information source can help generate more accurate SAV rules
  - Operators are allowed to specify how to use the SAV-related information in the SIB by their local configurations
Inter-domain SAVNET Architecture

- Basic idea
  - Consolidate SAV-related information from multiple sources and generate SAV rules based on the SAV-related information

- Main components
  - SAV-related information sources
  - SAV Information Manager (SIM)
  - SAV Information Base (SIB)
  - SAV table
SAV Table

- Data structure of SAV table

  Each row (i.e., SAV rule) records the most accurate incoming interfaces for each learned source prefix

<table>
<thead>
<tr>
<th>Index</th>
<th>Prefix</th>
<th>AS-level Interface</th>
<th>Direction</th>
<th>Information Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>P1</td>
<td>Itf.1</td>
<td>Provider</td>
<td>Collaborative Message, Routing Information Message</td>
</tr>
<tr>
<td>1</td>
<td>P1</td>
<td>Itf.2</td>
<td>Provider</td>
<td>Routing Information Message, RIB</td>
</tr>
<tr>
<td>2</td>
<td>P2</td>
<td>Itf.2</td>
<td>Provider</td>
<td>Manual Configuration</td>
</tr>
<tr>
<td>3</td>
<td>P3</td>
<td>Itf.3</td>
<td>Peer</td>
<td>Collaborative Message, RPKI ROA objects, RPKI ASPA objects</td>
</tr>
<tr>
<td>4</td>
<td>P4</td>
<td>Itf.4</td>
<td>Customer</td>
<td>Collaborative Message</td>
</tr>
<tr>
<td>5</td>
<td>P4</td>
<td>Itf.5</td>
<td>Customer</td>
<td>Routing Information Message, RIB</td>
</tr>
<tr>
<td>6</td>
<td>P5</td>
<td>Itf.5</td>
<td>Customer</td>
<td>Routing Information Message, RIB</td>
</tr>
</tbody>
</table>

SAV Table for AS X

<table>
<thead>
<tr>
<th>Source Prefix</th>
<th>Incoming Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Itf.1</td>
</tr>
<tr>
<td>P2</td>
<td>Itf.2</td>
</tr>
<tr>
<td>P3</td>
<td>Itf.3</td>
</tr>
<tr>
<td>P4</td>
<td>Itf.4</td>
</tr>
<tr>
<td>P5</td>
<td>Itf.5</td>
</tr>
</tbody>
</table>
By checking the source address and the actual incoming interface of each packet against the SAV table, the validity state of each packet can be considered “valid”, “invalid”, or “unknown”

- Packets with “valid” state should be permitted
- Packets with “invalid” state should be blocked
- Packets with “unknown” state can be blocked or permitted according to the SAV configurations

More details about how to use the SAV table can be found in [draft-huang-savnet-sav-table]
Considerations

- **Working in partial deployment**
  - Some information sources may not provide SAV-related information for all source prefixes in partial deployment scenario
  - New Inter-domain SAV mechanisms must support partial deployment

- **Security considerations**
  - Using active collaboration information faces the same security threats as those of BGP, including session security threats and content security threats
  - Existing BGP security mechanisms can be used to secure Collaborative Protocols
    - An independent security mechanism is needed when some BGP security mechanisms are not widely deployed
Conclusion

- Define the high-level inter-domain SAVNET architecture
  - Use SAV-related information from multiple sources to generate accurate SAV rules

- Leave open design space for new SAV mechanisms
  - How to select appropriate information sources?
  - How to collect and update the needed SAV-related information from selected sources?
  - How to use the SIB to identify the most accurate incoming interfaces?
Next Step

- Solicit comments and refine the draft
  - Many thanks to Igor Lubashev for the helpful revision suggestions
  - Your comments are welcome!

- Seek cooperation
  - Refining the draft
  - Detailed designs for the new inter-domain SAV mechanism
  - ......
Thanks!
Backup slides
Collaborative Messages

- Basic idea
  - The Collaborative Messages propagate or originate the real forwarding paths of prefixes between the Collaborative Protocol Speakers in different ASes

- The detailed designs for collaborative messages and protocol extensions are in the works
  - Seek cooperation
  - Carried out in the working groups responsible for the corresponding protocols
Three Validity States

- **“Valid”** means
  - There is a source prefix in SAV table covering the source address of the packet, and the valid incoming interfaces cover the actual incoming interface of the packet.

- **“Invalid”** means
  - There is a source prefix in SAV table covering the source address of the packet, but the actual incoming interface of the packet does not match any valid incoming interface.

- **“Unknown”** means
  - There is no source prefix in SAV table covering the source address of the packet.