SAVNET Architecture

draft-li-savnet-intra-domain-architecture

draft-wu-savnet-inter-domain-architecture

July 2023
Source Address Validation

- Source address validation (SAV) is important for defending against source address spoofing attacks.

- Since 2014, the MANRS initiative is calling on network operators to implement SAV as close to the source as possible.

- When an access network does not deploy SAV at the source (e.g., SAVI), intra- and inter-domain SAVs help block spoofed packets.

- Access SAV techniques are not in the analysis scope: such as RADIUS/DIAMETER, SAVI (e.g., IP Source Guard), Cable Source-Verify, etc.
Existing SAV Mechanisms

- ACL-based ingress filtering [RFC2827][RFC3704]
- Strict uRPF [RFC3704]
- Loose uRPF [RFC3704]
- FP-uRPF [RFC3704]
- VRF-uRPF [RFC8704]
- EFP-uRPF [RFC8704]
- Source-based RTBH filtering [RFC5635]

Common features: Primarily based on routing information (i.e., FIB/RIB) or manual configuration for generating SAV rules
Gap Analysis

- **Gap 1: Have operational challenges in dynamic or complex networks**
  - i) Manual updates induce high operational overhead (e.g., ACL for inbound filtering)
  - ii) They cannot work in all directions (i.e. interfaces) or scenarios

- **Gap 2: Have improper block or improper permit problems due to asymmetric routing**
  - Route: prefix P1 has next-hop Intf. 1
  - Reverse path: prefix P1 will come from Intf. 2

- More details in:
  - draft-ietf-savnet-intra-domain-problem-statement
  - draft-ietf-savnet-inter-domain-problem-statement
Design Goals

- **Goal 1: Automatic Update**
  - The routers after initial configurations can adapt to dynamic routing changes automatically, so that the operational overhead can be controlled.

- **Goal 2: Accurate Validation**
  - The real incoming interfaces of source prefixes need to be completely learned, and improper block can be avoided. By trying to exclude non-real incoming interfaces from the valid interface group, improper permit can be reduced.

- **Analysis:**
  - **Routing information** can be automatically updated but is **not enough** for generating accurate SAV rules.
  - The **information specifically useful to SAV** but may not useful for routing is **needed** for achieving the above goals.
SAV-Specific Information

- **SAV-specific information**: Explicitly or implicitly **indicate the accurate incoming direction of source addresses**, which helps routers generate accurate SAV rules. SAV-specific information is **specialized for SAV**.

- Examples of SAV-specific information
  - SAV rule, e.g., `<prefix, valid interfaces>`
  - Topology information, e.g., hidden prefixes
  - Forwarding information, e.g., real forwarding paths

- **SAV-specific information can replace or supplement routing information** when routers generate SAV rules.

- Both SAV-specific information and routing information are **SAV-related information**
Main Idea of SAVNET Architecture

**Main idea:** Besides routing information, allow routers or ASes to advertise SAV-specific information for automatically generate accurate SAV rules.

- **Now-1:** Generate SAV rule primarily based on routing information
  - Automatic but not accurate

- **Now-2:** Generate SAV rule based on manual configuration
  - Accurate but not automatic

- **Future:** Generate SAV rules based on SAV-specific information
  - Automatic and accurate

A simple example:

Routing information:
Prefix P1 has next-hop Intf. 1

SAV-specific information:
Prefix P1 will arrive at Intf. 2
- **Source Entity**: Advertise SAV-related information
- **Validation Entity**: Generate SAV rules and/or conduct validation validation
- **Communication channel**: Connect two entities for transmitting SAV-related information
- A device can act as a Source Entity, a Validation Entity, or both of them.

**Notes**: Take the figure of intra-domain architecture for illustration.
Messages carrying SAV-related Information

- Messages carrying SAV-related Information
  - SAV-specific information messages: Necessary for accurate SAV
  - Routing information messages: Necessary when SAV-specific information is not complete

- Multiple sessions:
  - The information can be delivered through multiple sessions of different protocols
  - A long-time session or a temporary one
  - Sufficient assurance of transmission reliability and timeliness
  - Authentication can be conducted before session establishment
How to Advertise Information

- Source Speaker/Validation Receiver

1. **Configuration Speaker/Receiver**
   - CLI, YANG, FlowSpec, and any other protocols for SAV

2. **Routing Protocol Speaker/Receiver**
   - OSPF, IS-IS, BGP, etc.

3. **SAV protocol Speaker/Receiver (new)**
   - Can be an extension to the routing protocol speaker
   - Used to advertise SAV-specific information
Connectivity Models

* The combinations of the above are also supported
Use Cases

**Case 1:** Help exchange asymmetrically advertised routes

Asymmetric routing in the Multi-homed Subnet Scenario

**Case 2:** Help automatically collect internal prefixes

Blocking Internal Prefixes at Internet Interfaces
**Use Cases**

**Case 3:** Advertise hidden prefixes (P3) that are not in routes

A direct server return (DSR) scenario

**Case 4:** Continue propagation of prefixes and discover “hidden” AS path

Limited propagation of prefixes caused by NO_EXPORT
More Details in the Drafts

- Refer to draft-li-savnet-intra-domain-architecture and draft-wu-savnet-inter-domain-architecture
  - SAV Agent
  - Deployment Considerations
  - Convergence Considerations
  - Manageability Considerations
  - Security Considerations
  - Privacy Considerations
The architecture is protocol-independent.

**Question**: Use which protocol to implement the architecture?

Existing SAV mechanisms mainly depend on routing information. Extending routing protocols for carrying SAV-specific information is an intuitive method.
- Routing protocol is the intuitive choice compared to existing Internet protocols

**How about a new protocol?**
- High efficiency like efficient packet encapsulation
- But, too much repetitive design, such as communication, negotiation, neighbor maintaining, and quality properties.
- Also, a new protocol is hard to deploy among ASes.
BGP Extensions for SAVNET?

- **Why BGP:**
  - Wide application scenarios and can work within an AS or among ASes
  - Easy to extend and provide good service isolation
  - Reuse existing basic design and quality attributes to reduce design and development workload and facilitate application
  - Explicit update and withdrawal without periodic flooding

- **How:**
  - **Much work to do:** how to carry, deployment problems, convergence challenges, manageability obstacles, security problems, privacy concerns, etc.
  - Need a detailed discussion on specific extension designs
Conclusion

- Give a brief introduction to the SAVNET architecture as well as some considerations.

- Since the work can be relevant to routing protocols like BGP, we would like to sync progress to IDR WG and solicit comments.

- Any comments are welcome. Also welcome to leave your comments in the idr or savnet mailing list.
Many thanks to the valuable comments from:

- Igor Lubashev
- Alvaro Retana
- Aijun Wang
- Joel Halpern
- Jared Mauch
- Kotikalapudi Sriram
- Rüdiger Volk
- Jeffrey Haas
- Xiangqing Chang
- Changwang Lin
- etc.
Thanks!