Considerations for SAV-specific information and the need of Traffic Origin Authorizations (TOAs)

Presenter: Lancheng Qin

July, 2025

What information does Inter-domain SAV need?

- Presume an AS receives a data packet with a given source address from a given external interface. SAV at the interface requires two categories of information:
  - Traffic Origin Information: Identify which ASes will source traffic using the given source address
  - Traffic Transit Information: Identify whether the interface is expected to receive traffic originated from the specific AS
- Advanced inter-domain SAV solutions typically use BGP updates and ROAs to obtain traffic origin information
  - EFP-uRPF (RFC8704, BCP84) obtains traffic origin information from BGP updates
  - BAR-SAV (draft-ietf-sidrops-bar-sav) additionally obtains traffic origin information from ROAs

Problem of Using BGP Updates and ROAs

- **Problem:** BGP updates and ROAs do not provide the complete traffic origin information for "hidden prefixes"
  - A hidden prefix refers to a prefix that an AS uses exclusively as a source address for sending traffic, without announcing a corresponding route to it in BGP
    - E.g., DSR technology, IP multicast, and satellite network scenarios (see [1, 2])
- In such cases, the corresponding IP address holder may intentionally choose not to register a ROA for the AS (which will NEVER announce a route to the hidden prefix)
- If SAV fails to discover all traffic origins of the hidden prefix by using BGP updates or ROAs
  - It may drop the legitimate traffic (see [3])

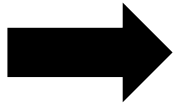
[1] https://mailarchive.ietf.org/arch/msg/savnet/8ywh8naVitPkiLR-e-Cc1T5E4Gw/
[2] https://mailarchive.ietf.org/arch/msg/savnet/pbc3jtv51-Y30M6dZrYYxnzm3pk/
[3] draft-ietf-savnet-iner-domain-problem-statement

The Necessity of Traffic Origin Authorization (TOA)

- SAV needs traffic origin information
  - SAV requires a mapping between a prefix and the ASes that are permitted to source traffic using the prefix as the source IP address
- The traffic origin may not be a route origin
  - No existing information source (e.g., BGP updates, ROAs, IRR route objects) provides traffic origin information when it differs from route origin
- A new mechanism is needed to enable IP holders to explicitly authorize ASes to source traffic from a prefix — even without announcing it in BGP

How to Implement the TOA Functionality

- Approach #1: Define a new RPKI signed object for TOA
  - ◆Clear semantic boundaries
  - ◆Avoids unintended side effects on the existing ROA



Preferred approach after consulting ASN.1 experts

- Approach #2: Extend the semantic of an existing ROA field
  - ◆Potentially easier to implement and deploy
  - ◆Risk of affecting the existing ROA

Considerations of TOA Usage

- Avoid redundancy
  - No need to register TOAs for information already covered by ROAs
  - Helps reduce RPKI object count and system overhead
- When is a TOA needed?
  - To authorize a traffic origin that is not a route origin
  - To explicitly signal that ROA-listed route origins are the only traffic origins
- SAV uses ROAs and TOAs
  - To derive the complete set of traffic origins for a prefix

Open Discussion