A Profile of **Si**gned **S**AVNET-**P**eering **I**nformation (SiSPI) Object for Deploying Inter-domain SAVNET

draft-chen-sidrops-sispi-00

Li Chen , Libin Liu , Dan Li*, Lancheng Qin*

Zhongguancun Laboratory and *Tsinghua University

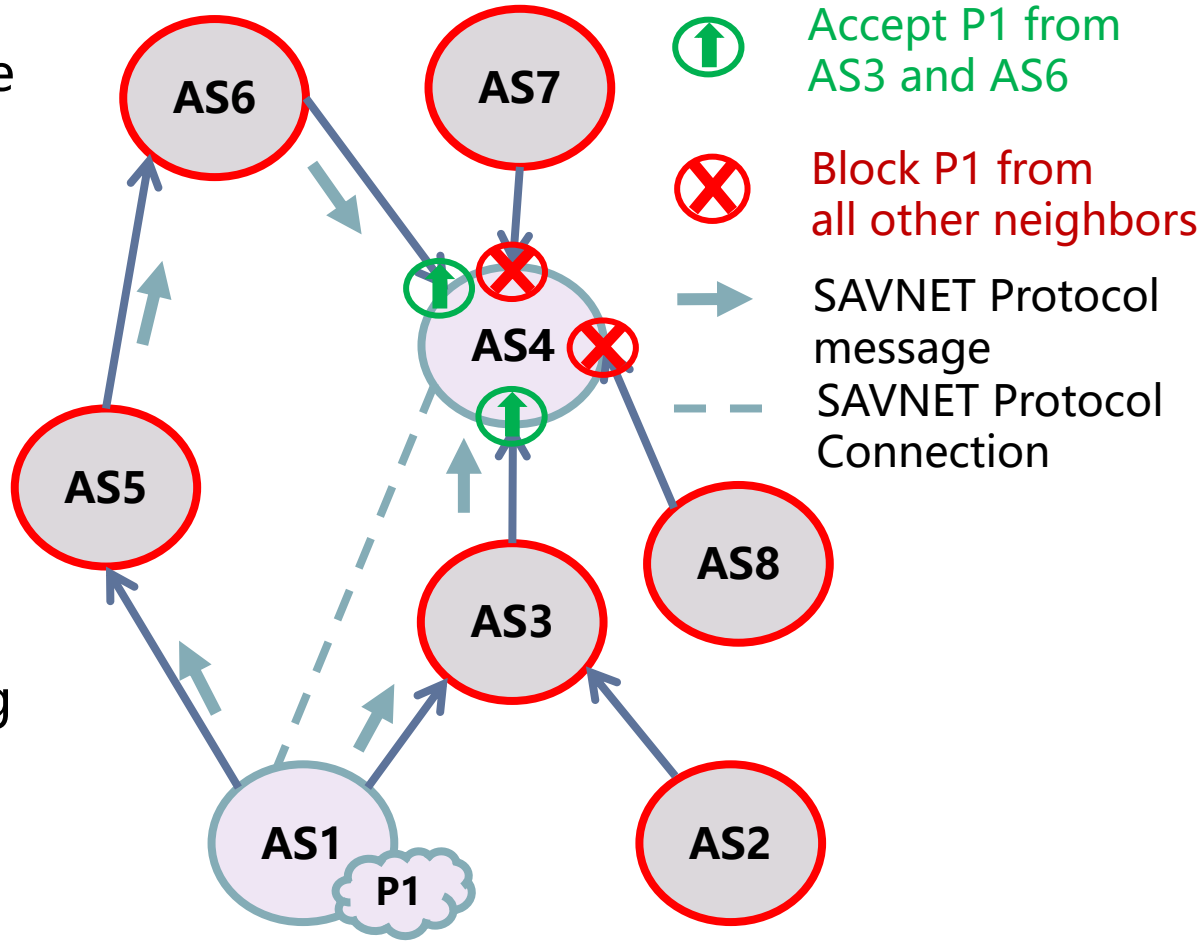
Background: Inter-domain SAVNET

- Attacks based on source **IP address spoofing**, such as reflective DDoS and flooding attacks, continue to present significant challenges to Internet security.
- Mitigating these attacks in inter-domain networks requires effective source address validation (SAV).
- While BCP84 offers some SAV solutions, such as ACL-based ingress filtering and uRPF-based mechanisms, existing inter-domain SAV mechanisms have limitations in terms of validation accuracy and operational overhead in different scenarios.
- Inter-domain SAVNET proposes to exchange SAV-specific information among ASes to solve the problems of existing inter-domain SAV mechanisms.
- SAV-specific information exchanging protocols (or SAVNET protocols for short) are shown to achieve higher validation accuracy and lower operational overhead in large-scale emulations.
  - https://datatracker.ietf.org/meeting/118/materials/slides-118-savnet-emulations-of-nine-sav-mechanisms-with-sav-open-playground-00

Background: SAVNET Protocol Description

- Main idea
  - Origin AS advertises its preferred AS paths to other ASes by SAVNET messages
  - Other ASes learn the incoming directions of the origin AS through received SAVNET messages
- Example: SAVNET protocol in action
  - AS1 and AS4 set up a SAVNET connection
  - AS1 selects AS path [AS1, AS3, AS4] and [AS1, AS5, AS6, AS4]
  - AS1 sends SAVNET messages to tell AS4 the paths
  - AS4 learns that AS3 and AS6 are valid incoming directions for P1, and all other neighbors are invalid

Relationships of AS4 and its neighbors: any one of c2p, p2c, or p2p



Problem Statement & Potential Solutions

- Key issue with Inter-domain SAVNET for operators: **Incremental Deployment**
  - Protocol-speaking agents (or SAVNET agents) within the SAVNET-adopting ASes need to find and establish connections with other SAVNET agents.
  - Currently, the peering is assumed to be **manual**.
    - Operationally (Cognitively) expensive. Learning curve for operators.
    - No incentive for newly adopting ASes: SAVNET peering must be negotiated one-by-one.
- Potential solutions for automatic SAVNET peering
  - Gossiping and flooding protocol
    - Bandwidth and computationally expensive.
  - A public registry that contains all ASes which both deploy SAVNET and are willing to setup SAVNET peering relationships.
    - A newly adopting AS can use this registry as a reference, and pick appropriate ASes to setup SAVNET peering relationship.
    - **RPKI is the most suitable choice for its central role in routing security.**

SiSPI Object Proposal

- The SiSPI Content Type
  - The content-type for a SiSPI object is defined as SAVNETAuthz, which has the numerical value of 1.2.840.113549.1.9.16.1.52.
- The SiSPI eContent
  - The content of a SiSPI object identifies a single AS that has deployed SAVNET for inter-domain SAV.
  - The eContent of a SiSPI object is an instance of SAVNETAttestation, formally defined by the following ASN.1 module:

```
SAVNETAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  asID          ASID,
  address       IPAddress }

ASID ::= INTEGER (0..4294967295)
IPAddress ::= BIT STRING
```

The asID field contains the AS number that has deployed SAVNET and can perform SAV on the data plane.

The IPAddress field stores the router's IP address within the AS whose ID is asID, which is utilized for establishing SAVNET connections.

Validating SiSPI Object

To validate a SiSPI object, the relying party MUST perform all the validation checks specified in RFC6488 as well as the following additional specific validation steps of the SiSPI object.

- The AS Identifier Delegation Extension [RFC3779] MUST be present in the end-entity (EE) certificate (contained within the SiSPI object), and the asID in the SiSPI object eContent MUST be contained within the set of AS numbers specified by the EE certificate's AS Identifier Delegation Extension.
- The EE certificate's AS Identifier Delegation Extension MUST NOT contain any ''inherit'' elements.
- The IP Address Delegation Extension [RFC3779] MUST be absent.

Using SiSPI Object

A router can use the AS_Path from BGP announcements, ASPA objects, and SiSPI to find the closest ASes to set up SAVNET peering:

1. **Closest AS Determination**:
   - Identify the ASes that frequently appear on the preferred paths to various destinations, implying they are topologically 'close' or significant transit providers.
   - Among these ASes, prioritize those that have a direct provider-customer relationship with the local AS (as indicated by ASPA objects), since they are potentially the closest peers.
2. **SiSPI Objects Utilization:**
   - Retrieve SiSPI objects from the RPKI repository to determine which ASes have deployed SAVNET.
   - Filter the previously identified closest ASes by checking whether they have a valid SiSPI object, which would indicate their readiness to establish SAVNET peering.
3. **Peering Candidates Selection:**
   - From the set of closest ASes with valid SiSPI objects, select candidates for SAVNET peering.
   - The selection criteria may include additional factors such as existing peering policies, traffic volumes, and peering agreements.

Thanks!

- Any comments?