A Profile of Signed SAVNET-Peering Information (SiSPI) Object for Deploying Inter-domain SAVNET

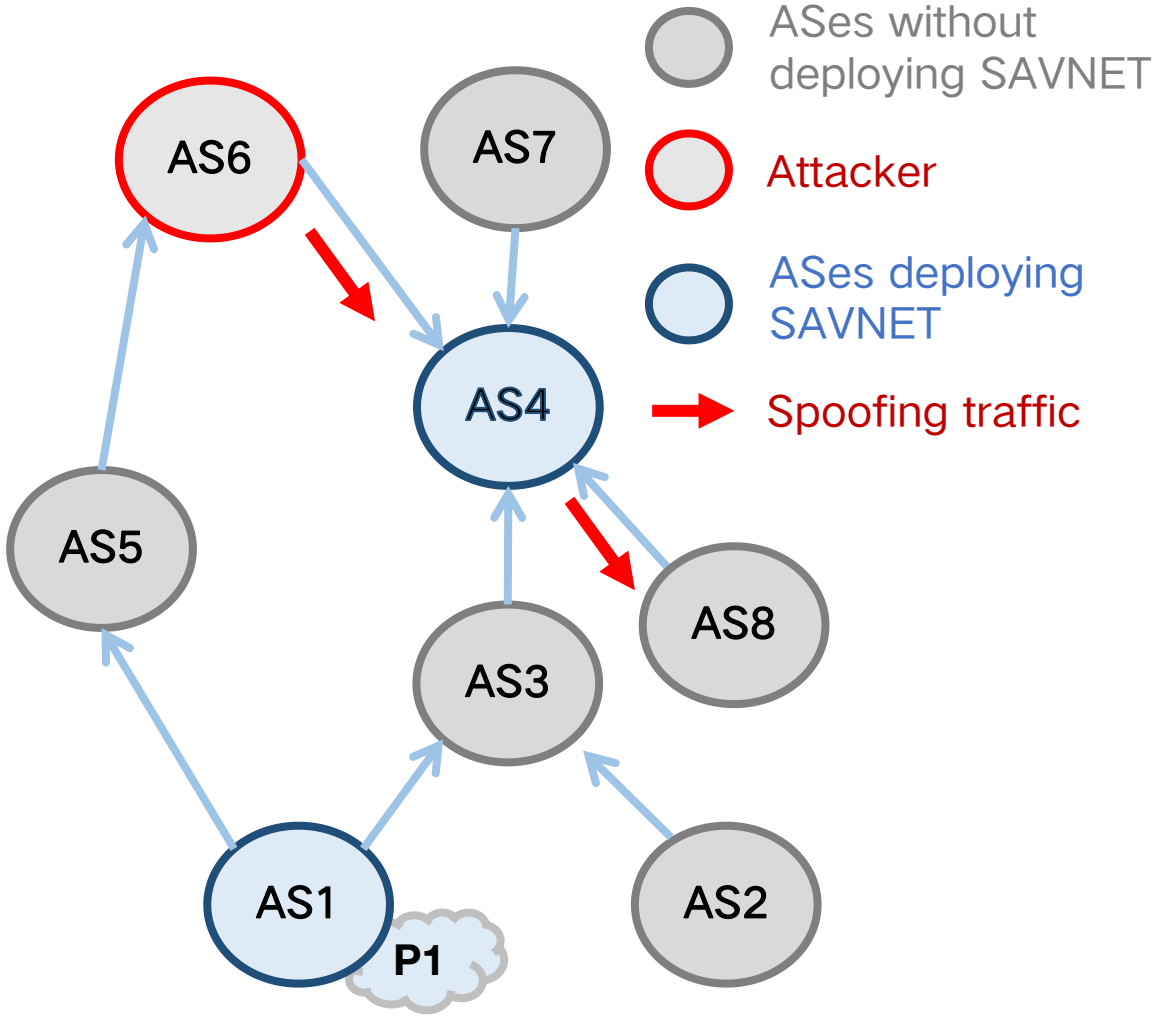
draft-chen-sidrops-sispi-02

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

Zhongguancun Laboratory and *Tsinghua University

Background: SiSPI Object

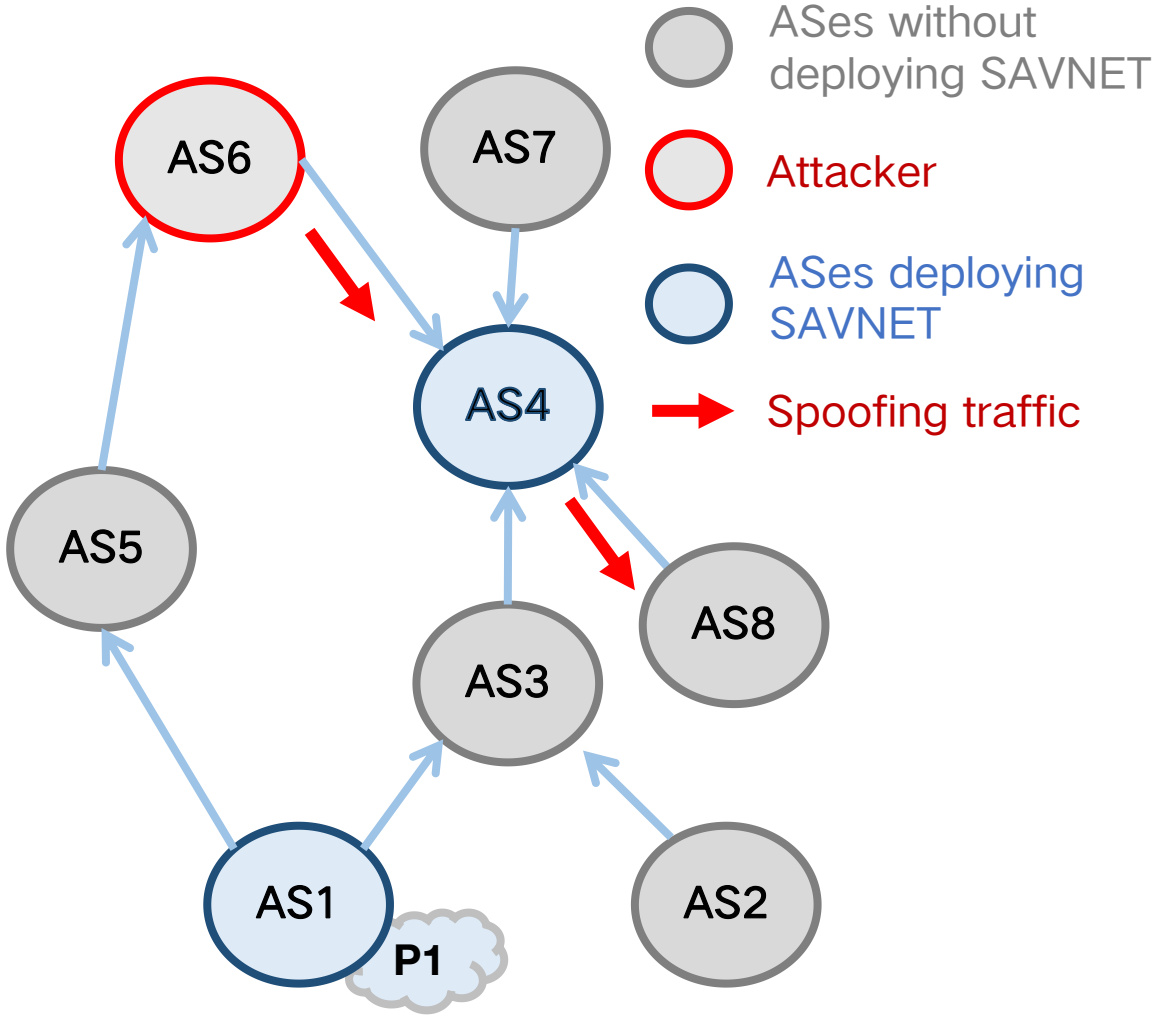
- **Remote peering is needed** for a SAVNET-adopting AS exchanging SAV-specific information with a remote AS in the partial deployment
  - An AS whose source prefix is spoofed and its neighbours may not be on the path of the spoofing traffic.
  - An AS can use the SAVNET-adopting ASes near the attacker to filter spoofing traffic.
- It can scale for exchanging SAV-specific information between ASes as more ASes deploy SAVNET following the operation recommendations
  - Limiting the maximum number of SAVNET peering connections for an AS.
  - Leveraging connected peering SAVNET-adopting ASes as the agents for forwarding the information instead of a direct connection.



All AS relationships in upward direction are C2P.

Background: SiSPI Object

- SiSPI is needed for automatic peering
  - SAVNET agents of the SAVNET-adopting ASes, such as AS 1 and AS 4, need to find other SAVNET-adopting ASes and determine the ones to establish connections.
  - Automatic SAVNET peering can help reduce the operational overhead and accelerate the process of connection establishment.
- SiSPI proposes a public RPKI 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.



All AS relationships in upward direction are C2P.

Summary of Comments

- Comments on **ASN.1 module** of the eContent of SiSPI object (Russ Housley)

1. The ASN.1 in the document is incomplete and cannot be compiled.
2. Russ is concerned that the authors are reusing the name ADDRESS-FAMILY from other drafts. They are using it differently and are providing a list of IP addresses, not a list of prefixes. Russ suggests a different class name.
3. Russ provides an ASN.1 module that compiles.
4. Note that two OIDs are needed, so if the authors want to use this module, the IANA considerations need to be updated.

Summary of Main Updates

- Revise the SiSPI Content Type Section
  - Revise the name of the content-type for a SiSPI object from “SAVNETAuthz” to “id-ct-rpkiSiSPI”.
- Revise the SiSPI eContent Section
  - Revise the ASN.1 module to update the class name “ADDRESS-FAMILY”, the names of corresponding elements, and the format of the ASN.1 module.
- Revise the SiSPI Validation Section
  - Add an additional validation step for a SiSPI object “The contents of the CMS eContent field MUST adhere to all the constraints described in Section 2.”.
- Revise the IANA Considerations Section
  - Add the reference for RPKI signed object registry and add a new subsection

Updates of SiSPI Object eContent

- The eContent of a SiSPI object is formally defined by the ASN.1 module:

Update the format of ASN.1 module to make it be compiled correctly.

Element **IPFamilyAddresses** contains a SEQUENCE which contains one instance of ipFamily and one instance of ipAddresses.

The element **IPAddress** is length bounded through the information object class IP-Address-FAMILY and its type is a BIT STRING.

```
RpkiSiSPI-2024
     { iso(1) member-body(2) us(840) rsadsi(113549)
       pkcs(1) pkcs9(9) smime(16) mod(0)
       id-mod-rpkiSiSPI-2024-2024(TBD0) }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS
  CONTENT-TYPE
  FROM CryptographicMessageSyntax-2010 -- in [RFC6268]
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
      pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) } ;

ct-rpkiSiSPI CONTENT-TYPE ::=
  { TYPE SAVNETAttestation IDENTIFIED BY id-ct-rpkiSiSPI }

id-ct-rpkiSiSPI OBJECT IDENTIFIER ::=
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) id-smime(16) id-ct(1) TBD1 }

SAVNETAttestation ::= SEQUENCE {
  version [0]   INTEGER DEFAULT 0,
  asID          ASID,
  addresses     SEQUENCE OF IPFamilyAddresses }

ASID ::= INTEGER (0..4294967295)

IPFamilyAddresses ::= SEQUENCE {
  ipFamily    IP-ADDRESS-FAMILY.&afi ({IPAddressFamilySet}),
  ipAddresses IP-ADDRESS-FAMILY.&IPAddresses ({IPAddressFamilySet}{@ipFamily}) }

IP-ADDRESS-FAMILY ::= CLASS {
    &afi          OCTET STRING (SIZE(2)) UNIQUE,
    &IPAddresses
  } WITH SYNTAX { AFI &afi IP &IPAddresses }

IPAddressFamilySet IP-ADDRESS-FAMILY ::= { ipAddressFamilyIPv4 | ipAddressFamilyIPv6 }

ipAddressFamilyIPv4 IP-ADDRESS-FAMILY ::= { AFI afi-IPv4 IP IPv4Addresses }

ipAddressFamilyIPv6 IP-ADDRESS-FAMILY ::= { AFI afi-IPv6 IP IPv6Addresses }

afi-IPv4 OCTET STRING ::= '0001'H

afi-IPv6 OCTET STRING ::= '0002'H

IPv4Addresses ::= SEQUENCE (SIZE(1..MAX)) OF IPAddress{ub-IPv4}

IPv6Addresses ::= SEQUENCE (SIZE(1..MAX)) OF IPAddress{ub-IPv6}

ub-IPv4 INTEGER ::= 32

ub-IPv6 INTEGER ::= 128

IPAddress {INTEGER: ub} ::= BIT STRING (SIZE(0..ub))

END
```

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

The field of **ipFamily** contains an OCTET STRING which is either ‘0001’ H (IPv4) or ‘0002’ H (IPv6).

The field of **ipAddresses** contains a SEQUENCE of IPAddress instances.

Updates of IANA Considerations

- Add the reference for RPKI signed object registry
  - Please add an item for the SiSPI object file extension to the RPKI as follows:

Name	OID	Reference
Signed SAVNET-Peering Information	1.2.840.113549.1.9.16.1.52 (suggested)	draft-chen-sidrops-sispi

- Add a new subsection “SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)”
  - IANA is requested to allocate the following in the "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" registry:

Decimal	Description	Reference
TBD	id-mod-rpkiSiSPI-2024-2024	draft-chen-sidrops-sispi

Thanks!

- We are going to implement SiSPI.
- Any comments?