An RPKI and IPsec-based AS-to-AS Approach for Source Address Validation

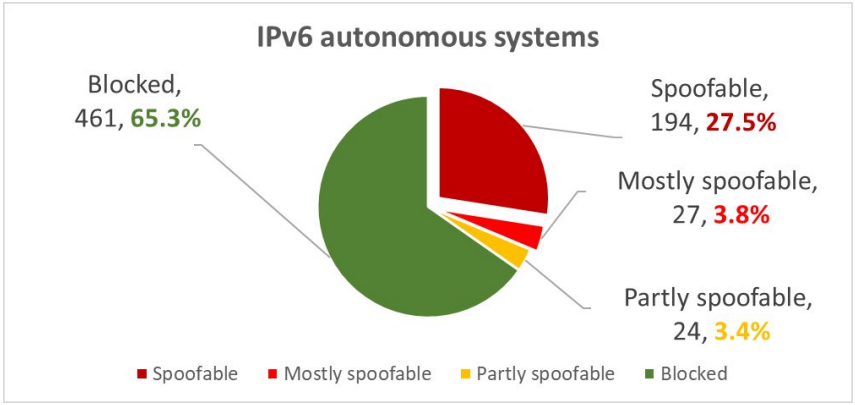
draft-xu-ipsecme-risav-00: https://datatracker.ietf.org/doc/draft-xu-ipsecme-risav/
Github: https://github.com/bemasc/risav/

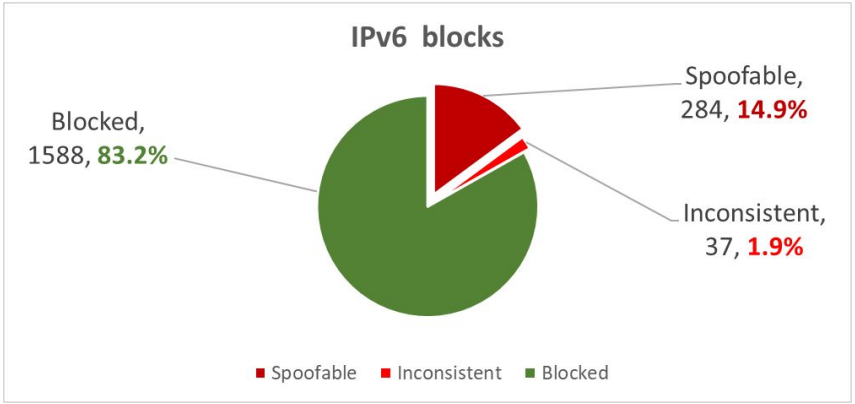
SAV question definition

Vulnerability: It is difficult to resist attacks by disabling the IP source address.

Traceability: Attackers could conceal location and identity.

Manageability: It is difficult to realize billing and other management through the IP source address.

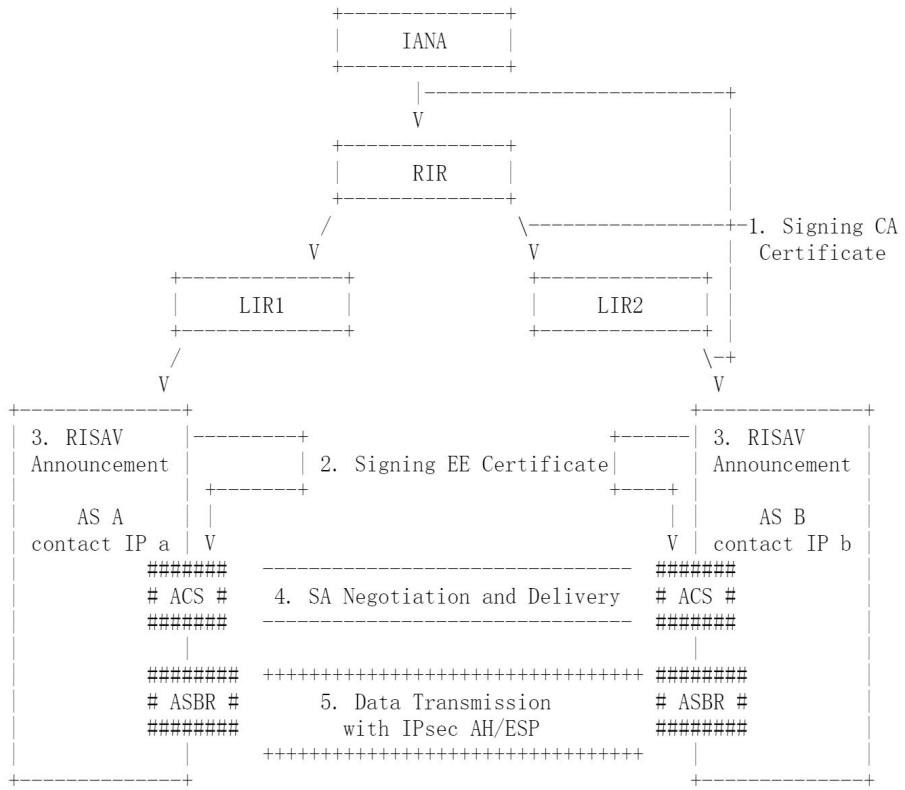




REF: https://spoofer.caida.org/summary.php

Overview

- cryptographically-based inter-AS SAV protocol
- RPKI + IPsec compatible
- add MAC at source ASBR and delete it at destination ASBR



Control plane

Enabling RISAV

- Announcing that this AS supports RISAV.
- Publishing contact IPs.
  - RISAVAnnouncement: a Signed Object, testing for indicating the reliability of contact IP.

```
RISAVAnnouncement ::= SEQUENCE {
        version [0] INTEGER DEFAULT 0,
        asID ASID,
        contactIP ipAddress,
        testing BOOLEAN }
```

- Performing IPsec session initialization (i.e. IKEv2).

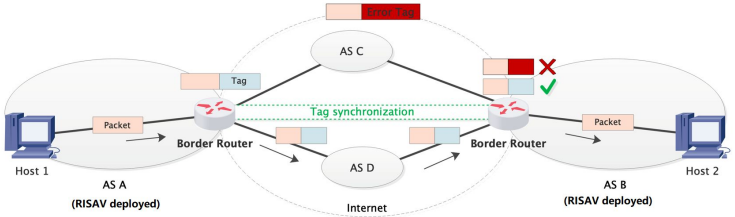
Green Channel

- A channel established only between pair ACSes.
- For rebooting quickly and imperceptible
- When it enabled, ASBRs don't perform RISAV validation.

Disabling RISAV

- Targeted Shutdown
  - NO pair of inbound-outbound SAs. => strictly unidirectional SA.
  - If one AS sends NO_ADDITIONAL_SAS to its peer, it means the peer MUST halt all further RISAV negotiation temporarily.
  - Deleting all SAs and rejecting new ones.
- Total Shutdown
  - Apply a targeted shutdown
  - Stop requiring RISAV authentication of incoming packets.
  - Remove the "RISAVAnnouncement" from the RPKI Repository.
  - Wait at least 24 hours.
  - Shut down the contact IP.

Data plane



Transport mode

```
                    1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Next Header   | Payload Len   |    RESERVED    |     Scope     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Security Parameters Index (SPI)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   Sequence Number Field                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+             Integrity Check Value-ICV (variable)              |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Updated AH Format.

- ONLY the “Scope” field, which identifies the scope of protection for RISAV AH, is different from the original AH.
  - 0 for IP and 1 for AS; others not defined.
- Only used for AS-to-AS communication
- Only indexed by SPI and counterpart ASN regardless of src IP or dst IP in SAD
- Transparent to the end hosts.

Tunnel mode

- ESP encapsulation
- Tunnel is built with current ASBR and ACS’s contact IP of another AS
- ASBR maintains its own SAD indexed by SPI and counterpart ASN

RISAV implementations **MUST** support transport mode, and **MAY** support tunnel mode.

- USE_TRANSPORT_MODE notification

MTU Handling and Replay Protection

Choose a **minimum** acceptable "**inner MTU**" and reject RISAV negotiations whose inner MTU is **lower than** inner MTU.

- Prior knowledge of the outer MTU
- Estimation of the outer MTU

ICMP PACKET TOO BIG(PTB)

- Transport Mode
  - MTU value reduced by the total length of RISAV AH header
- Tunnel Mode
  - Be treated as single IP hop
  - Oversize will cause generating PTB

MTU Estimation

- Initial estimation
  - PMTUD (RFC 7383)
- MTU monitoring

Traffic Selector and Replay Status

- Simplest RISAV Configuration
  - Single Child SA (**SHARING one**)
  - TSi lists all the IPs of sending AS
  - and TSr lists all the IPs of receiving AS

Enabling Replay Protection

- Sender creates many Child SAs and narrow the TSi.
- each SA is processed by a single receiving ASBR
- Tunnel Mode: route each SA to a specific ASBR using IKEv2 Active Session Redirect.
- Transport Mode:

Disabling Replay Protection

- Set the REPLAY-STATUS indication to False in CREATE_CHILD_SA notification,
- and delete the SA if….

AS IP Ranges

Others

Security Consideration

1. Threat model
   a. Reply attack
   b. Downgrade attack
2. Incremental benefit
3. Comparability
   a. IPsec
   b. Other SAVs

Operational Consideration

1. Reliability
2. Multiple ASBRs
3. Performance
4. NAT

Consistency with Existing Protocols

- IPv6
  - MTU: minimum of 1280B. {MTU-Handling}
  - Header Modification: RISAV-AH
  - IP address usage
- RPKI Usage
  - RISAV fully falls squarely within the limits of usage of RPKI key material.

Thanks

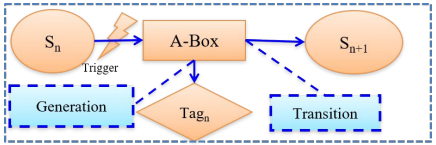
Possible Extensions

Header-only Authentication

It only authenticates the **IP source address**, **IP destination address**, etc.

An attacker could simply replace the payload, allowing it to issue an unlimited number of spoofed packets.

Time-base key rotation



Time triggers the SM transit from **S(n)** to **S(n+1)** following the algorithm defined by two parties as well as generating the tags as the side product.

Static-static ECDH negotiation

Ideas from RFC 6278

It would allow ASes to agree on shared secrets simply by syncing the RPKI database.

Pros.

- Stateless

Cons.

- Novel IPsec negotiation mechanism