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

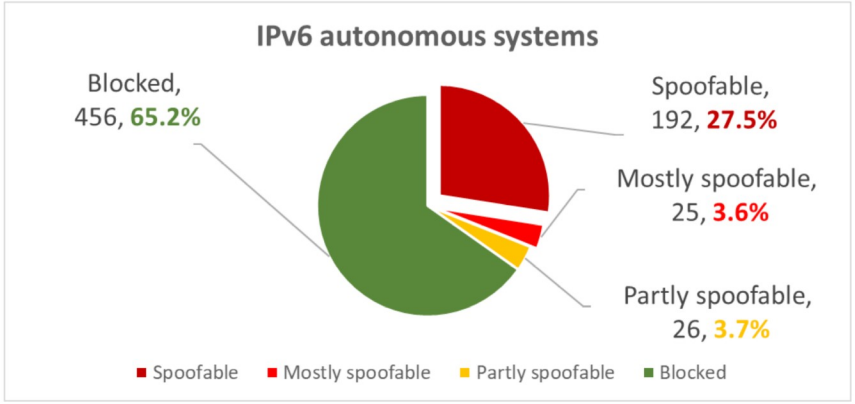
draft-xu-risav-02: https://datatracker.ietf.org/doc/draft-xu-risav/
Github: https://github.com/bemasc/draft-xu-risav/

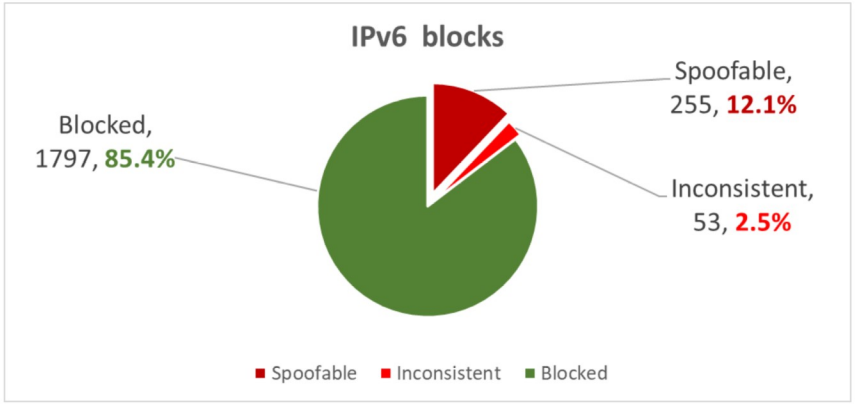
SAV question definition

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.

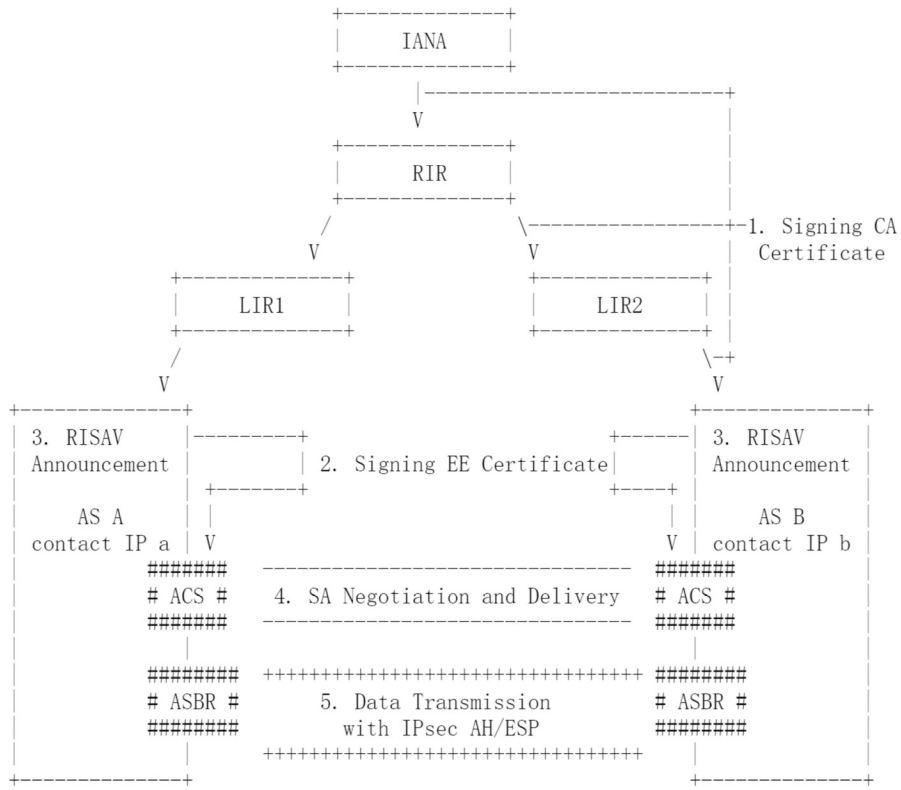




REF: https://spoofer.caida.org/summary.php

What RISAV is and how it works

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



Control plane

Enabling RISAV

- Announcing that this AS supports RISAV.
  - RISAVAnnouncement: testing for indicating the reliability of contact IP.
- Publishing contact IPs.
- Performing IPsec session initialization (i.e. IKEv2).

Disabling RISAV

- Stop requiring RISAV authentication of incoming packets.
- Remove the RISAVAnnouncement from the RPKI Repository.
- Wait at least 24 hours.
- Stop sending RISAV and shut down the contact IP.

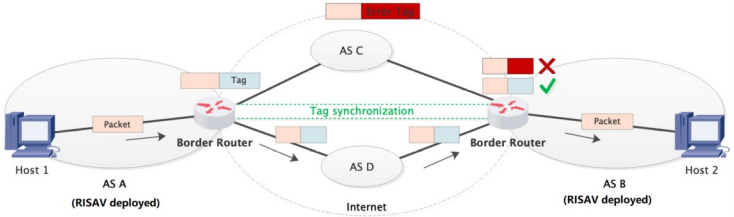
```
RISAVAnnouncement ::= SEQUENCE {
        version [0] INTEGER DEFAULT 0,
        asID ASID,
        contactIP ipAddress,
        testing BOOLEAN }
```

OPEN QUESTION:
Does IKEv2 have an authenticated permanent rejection option that would help here?

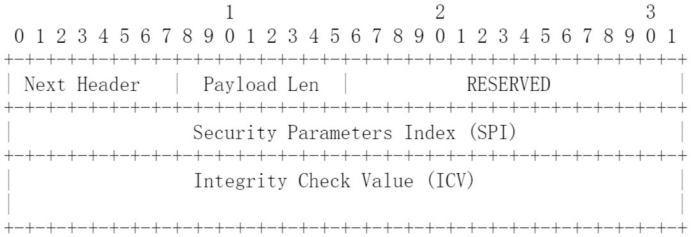
RFC 6023: CHILDLESS_IKEV2_SUPPORTED

IKEv2: TS_UNACCEPTABLE or
NO_PROPOSAL_CHOSEN

Data plane



Transport mode



- `Seq Num` field is omitted for this is presumed to be a `multi-sender SA`
- Only used for AS-to-AS communication
- Only indexed by SPI and counterpart ASN regardless of src IP or dst IP in SAD

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

PROBLEM: ICV in ESP is optional. ESP doesn't protect the source IP in default.

OPEN QUESTION: How do peers express a preference or requirement for transport or tunnel mode?

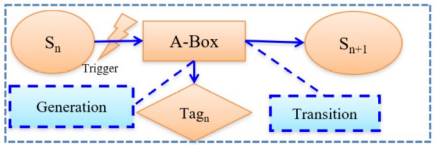
Possible Extensions

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

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. MTU
5. NAT

Open Questions

1. Does IKEv2 have an authenticated permanent rejection option that would help to disable RISAV normally and orderly?

2. How do peers express a preference or requirement for transport or tunnel mode?

3. PROBLEM: Can we negotiate an extension to ESP that covers the IP header? Or could we always send from the contact IP and encode the ASBR ID in the low bits of the SPI?

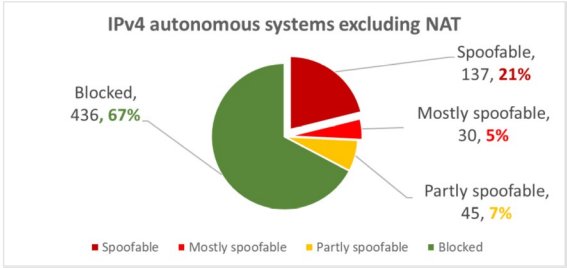
Thanks

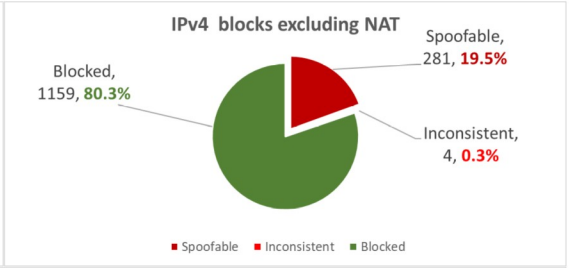
SAV question definition

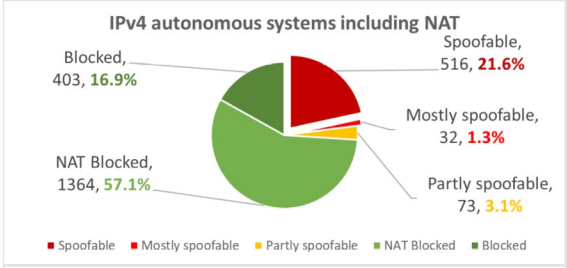
Vulnerability: It is difficult to resist attacks by disabling the IP source address.

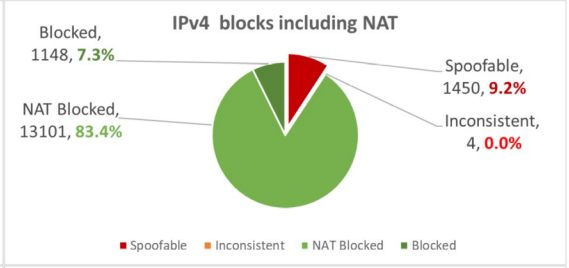
Traceability: Attackers could conceal location and identity.

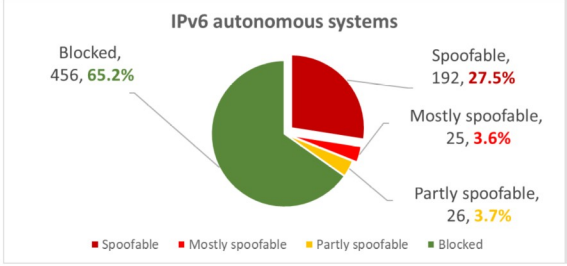
Manageability: It is difficult to realize billing and other management through the IP source address.

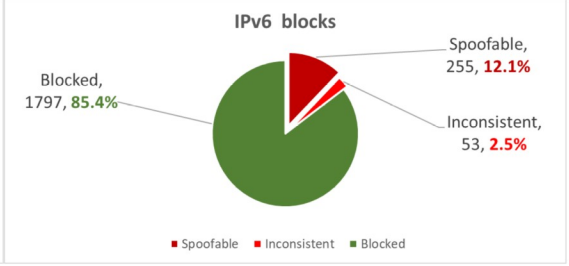












REF: https://spoofer.caida.org/summary.php