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

Ke Xu, Jianping Wu, Yangfei Guo, Benjamin M. Schwartz, Haiyang Wang

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

IETF 117 Jul. 2023
Site-to-site IPsec is awesome

- It defeats IP spoofing
  - Any packets arriving from the peer’s IP range without IPsec can be dropped.
- It improves security
  - IPsec makes traffic tamper-resistant.
- It improves privacy
  - IPsec tunnels allow (but do not require) encryption.
- It is well-understood and technically mature.
  - With IKEv2, etc.
- It can be extremely fast.
  - 1 Tbps IPsec ESP demonstrated in pure software in 2021.
- Any pair of networks can use it.
  - There’s no need for the participants to be direct BGP peers.
Hi Bob, this is Alice is from Corp1. Would you be interested in setting up a site-to-site tunnel with us? We have an IKEv2 gateway running at 2001::db8:1 (see attached certificate hash).

Hi Alice, that sounds great. We can get each other’s IP ranges from the RPKI database. We’ll authenticate IKEv2 with the attached client certificate, and use the tunnel for all traffic.
1. Define a config format equivalent to Alice & Bob’s emails.
2. Each participant publishes their config in the RPKI database.
3. All participants sync the RPKI database as usual.
4. Each participant connects to all the other participants.

Result: \(O(N^2)\) IPsec associations with \(O(N)\) human work.

This is the core idea of RISAV. Everything else is technical details, subject to change, to solve problems like:

- How do we make IPsec scale to serve networks with many gateways and sites without disrupting their routing?
- How do we minimize and tolerate MTU loss?
- Can make it easy and safe to turn the tunnel on and off?
**RISAV Overview**

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

**IP Source Address is viewed as correct only if the packet carries a correct MAC.**

**RISAV does not require encrypting the whole packet or not aim to defend a specific attack. It just aims to provide SAV.**
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.

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

- USE_TRANSPORT_MODE notification

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

Network-to-Network Data Plane
• RISAV treats the Internet as a true “network of networks”
• RISAV provides clear benefits for participants even when only fractionally deployed.
  • e.g. if x% of networks have RISAV, joining RISAV reduces your amplification-reflection attack volume by x% (on average).
• The design has been getting simpler as other IPsec drafts propose solutions to key protocol scalability challenges.
• Seeking working group adoption
  • IPSECME, SIDRops, or elsewhere?
• Suggestions are welcomed.
Thanks
SAV Problem Statement

- **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.

*This is not properly handled.*
Enabling RISAV

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

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.

Green Channel

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

RISAVAnnouncement ::= SEQUENCE {
  version [0] INTEGER DEFAULT 0,
  asID ASID,
  contactIP SEQUENCE (SIZE(1..2)) OF IPAddressFamily,
  testing BOOLEAN DEFAULT FALSE }

Control Plane
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
  - 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
**Possible Extensions**

### Time-base Key Rotation

![Diagram](#)

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.

### 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.

### 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
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.