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 118 Nov. 2023

What RISAV is and How it works

WHAT

An approach for inter-AS Source Address Validation with RPKI and IPSEC.

HOW

RPKI

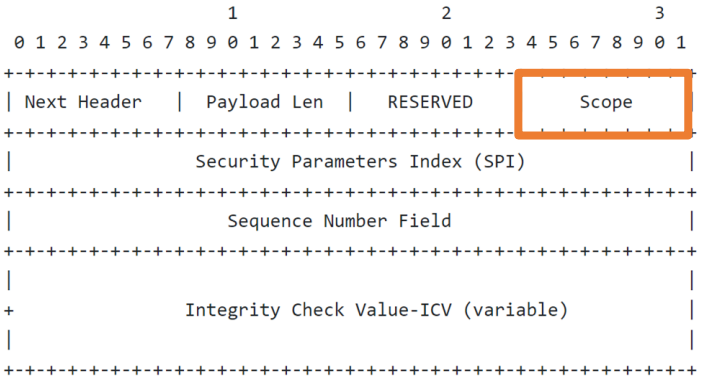
1. Define a config format for Contact IP and ASID.
2. Each participant publishes their config in the RPKI database.
3. All participants sync the RPKI database as usual.

IPSEC

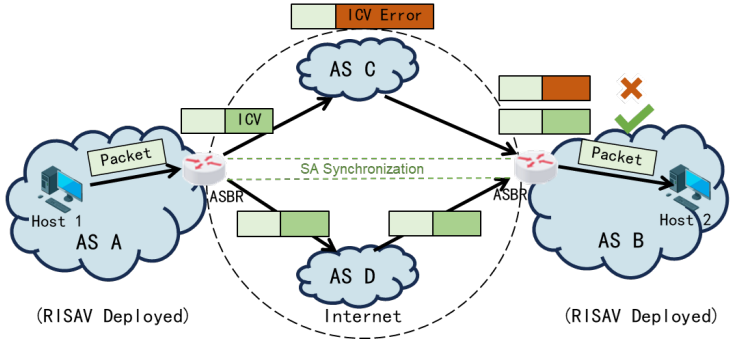
4. Each participant connects to all the other participants by IKE.
5. Data plane communicates with IPsec encapsulation.

COST: $O(N^2)$ IPsec associations with $O(N)$ human work.

Changes to IPsec



- AH
  - Reserved(2B) => Reserved(1B) + Scope(1B)
  - Scope identifies the scope of protection for RISAV AH.
    - 0 for IP and 1 for AS;
    - others are not defined
  - Only used for AS-to-AS communication
- IKE
  - Only indexed by SPI and counterpart ASN regardless of src IP or dst IP in SAD
- Transparent to the end hosts.



- ESP
  - Encryption
    - ESP Encryption
    - ESP_NULL Encryption
  - Tunnel is built with current ASBR and ACS's(AS Control Server) contact IP of another AS
- IKE
  - 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

Closing remarks

- *Changes are acceptable?*

- 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.
- Suggestions are welcomed.

Thanks