

Applying IPSec to Overlay routing

Jukka.Ylitalo@hut.fi

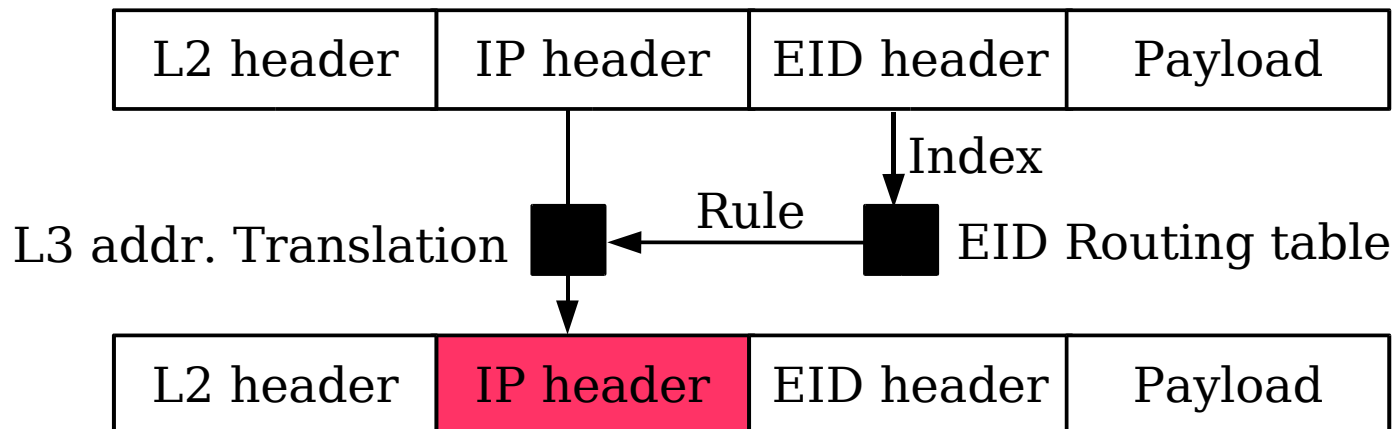
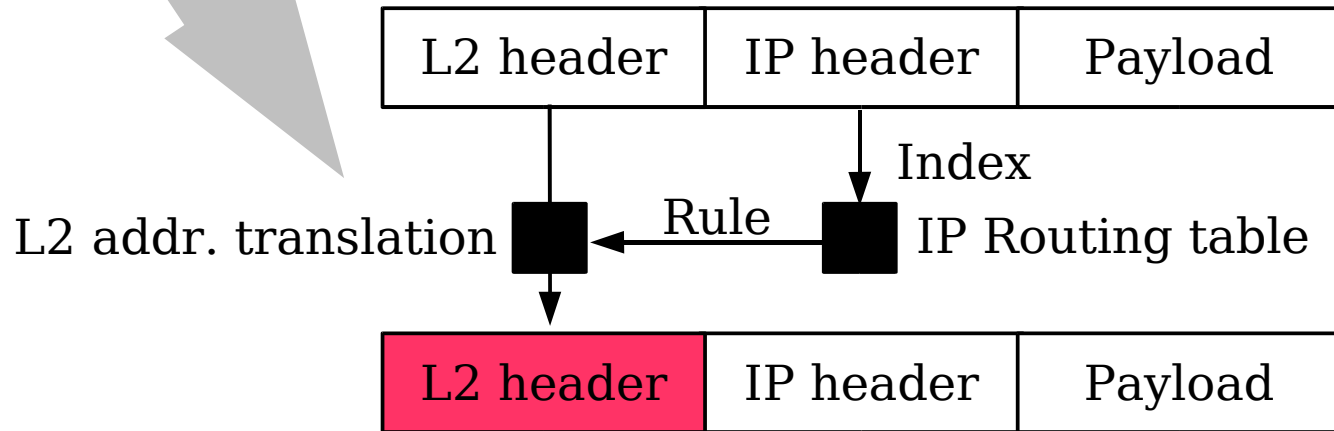
T-110.557 Research seminar on
telecommunications software

1.12.2004, HIIT

Legacy Routing vs. Overlay Routing

- Legacy IP routing and overlay are functionally similar, but at different layers in the stack.
- A legacy router translates link layer addresses.
- An overlay router translates network layer addresses.
- A legacy router uses the IP addresses as routing table identifiers, used to guide link layer address translation.
- The overlay routing uses uses end-point identifiers for network layer address translation.

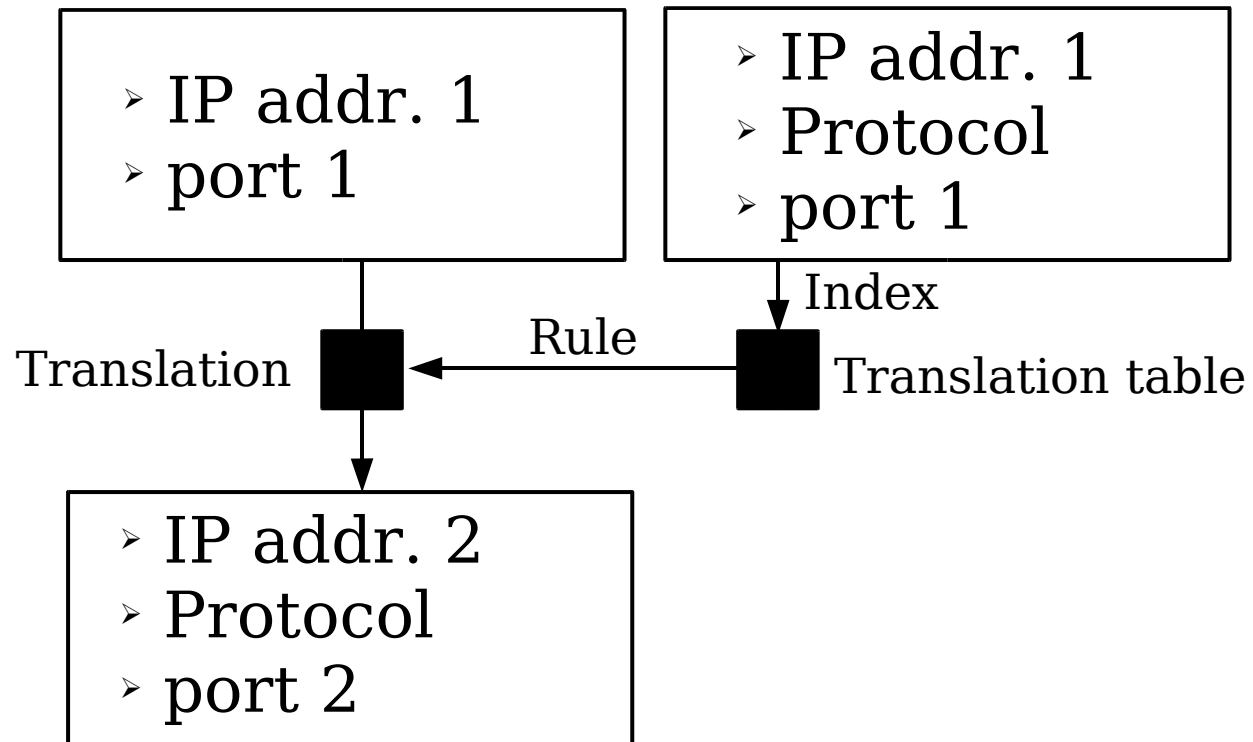
Legacy Routing vs. Overlay Routing



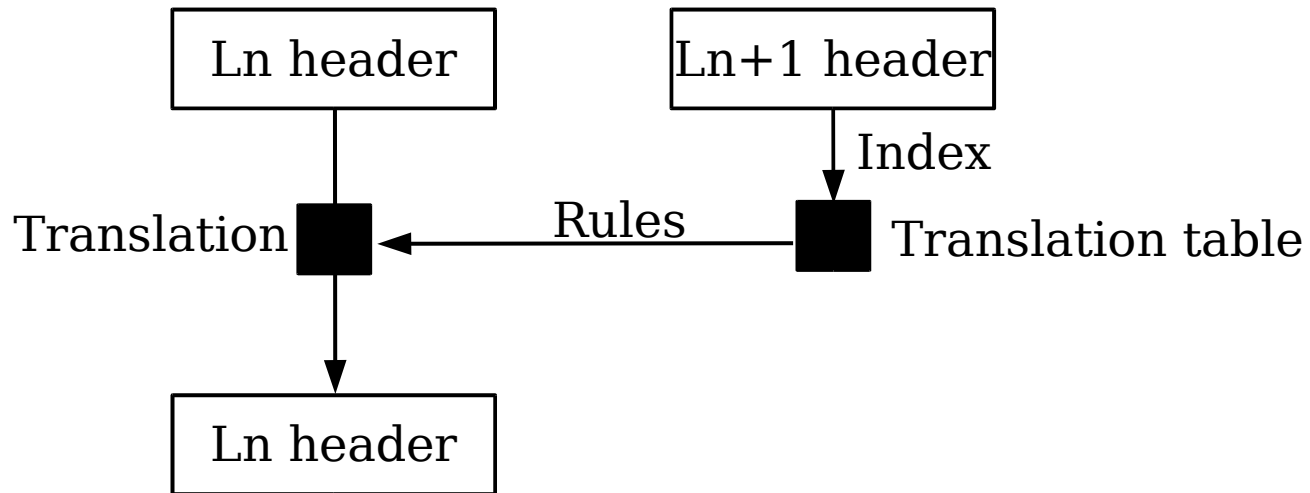
Overlay Routing vs. Network Address Translation (NAT)

- Our approach is based on the observation that NAT is similar to overlay routing.
- IP address translation is based on the end-point identifiers that are semantically separated from locators.
- Thus, IPSec NAT traversal problems must be tackled.

NAT



Generalization



- › L1 addr. translation = signal processing (bridging)
- › L2 addr. translation = routing
- › L3 addr. translation = NAT / overlay routing
- › L4 addr. translation = Delegation

Challenges in supporting IPSec in overlay routing

- Overlay routing hides the actual location of an end-host. I.e., implements NAT.
- Supports asymmetric routing. I.e., a host may send and receive packets via different overlay routers.
- As a result it is hard to name and identify end-to-end IPsec Security Associations (SAs).

SPI multiplexed NAT (SPINAT)

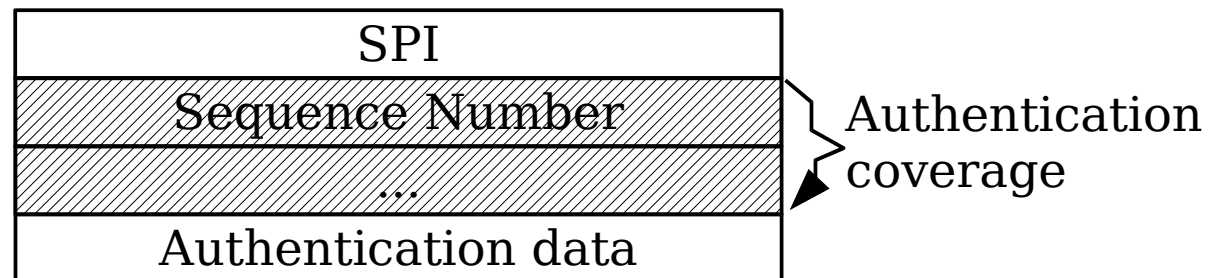
- When IPSec is used the Security Parameter Index (SPI) together with an IP-address -pair can work as an index for end-point identifiers.
- The address translation is based on the SPI value and IP addresses carried in the IPSec payload packets.

Changing SPI value

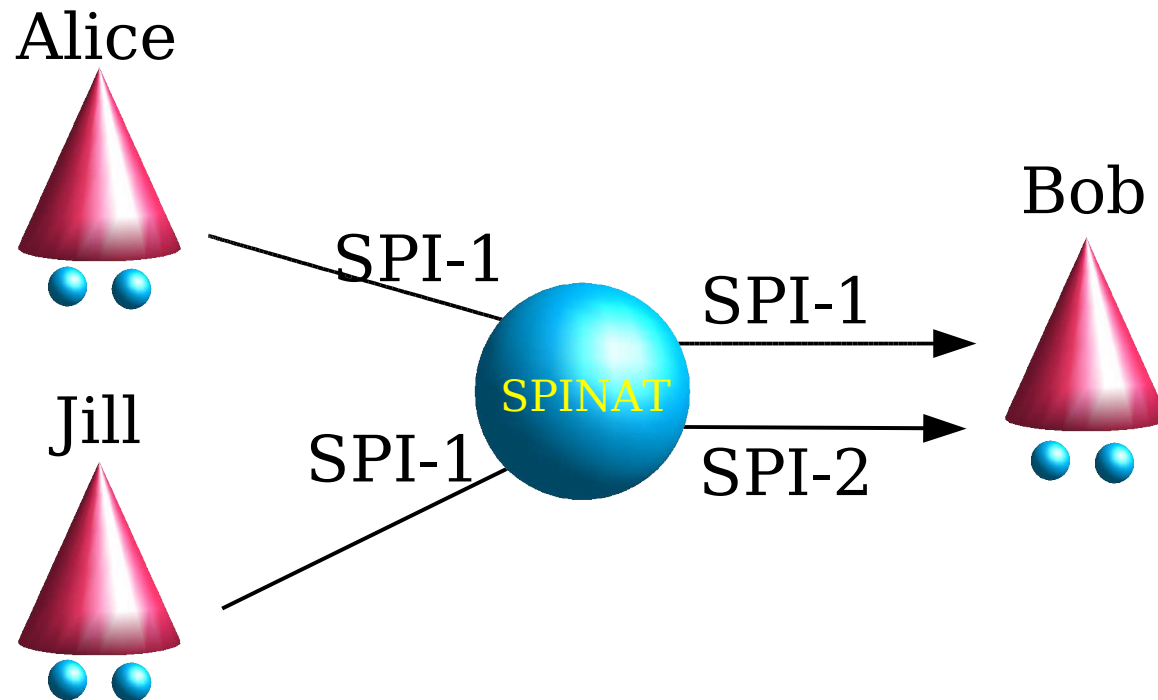
- The SPINAT device may change the SPI value.
- SPI values included in the key exchange and mobility management messages cannot be encrypted or included into the signature
- SPI values cannot be integrity protected in IPSec payload packets.

New IPSec sBEET mode

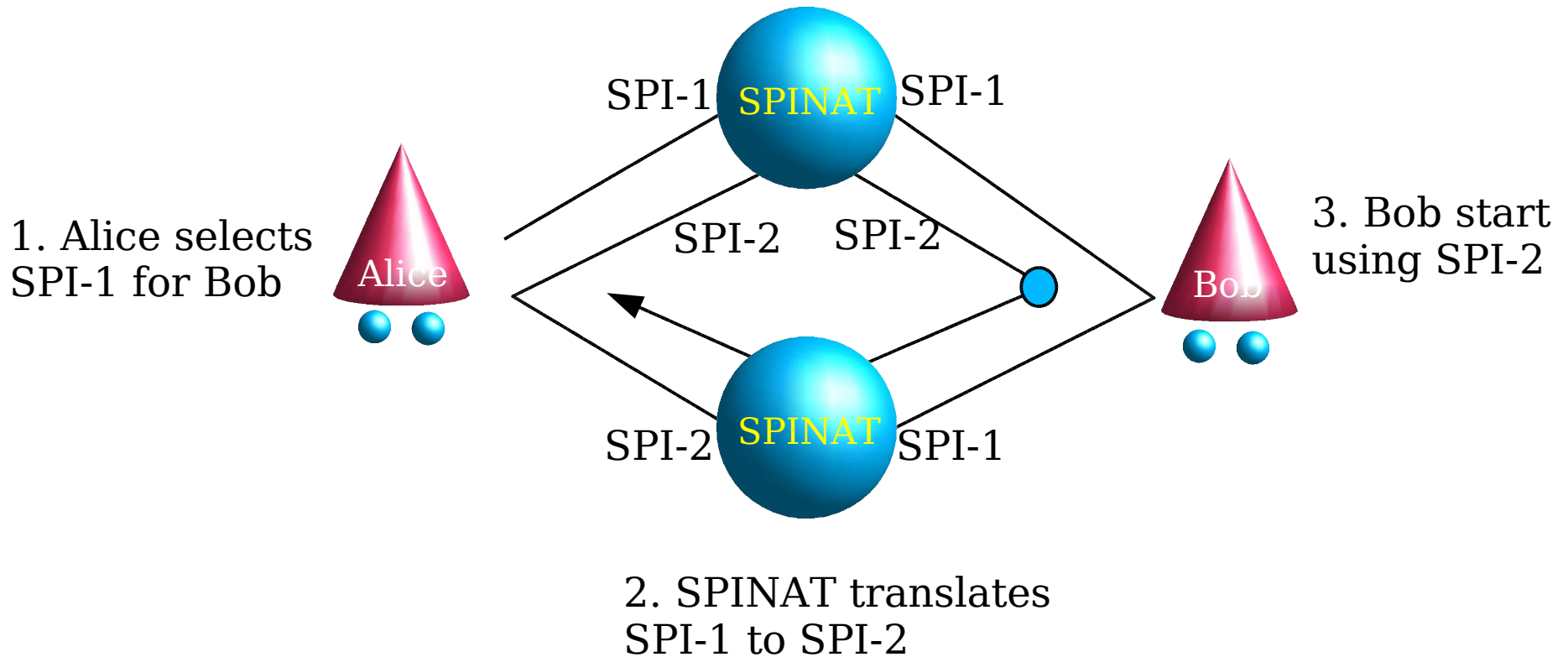
- › A stripped Bound End-to-End Tunnel (sBEET) mode
- › Uses transport mode packet format, but provides limited tunnel mode semantics (like BEET mode).
- › The sBEET mode does not include the SPI values in the ESP header integrity protection computation.



Symmetric communication path



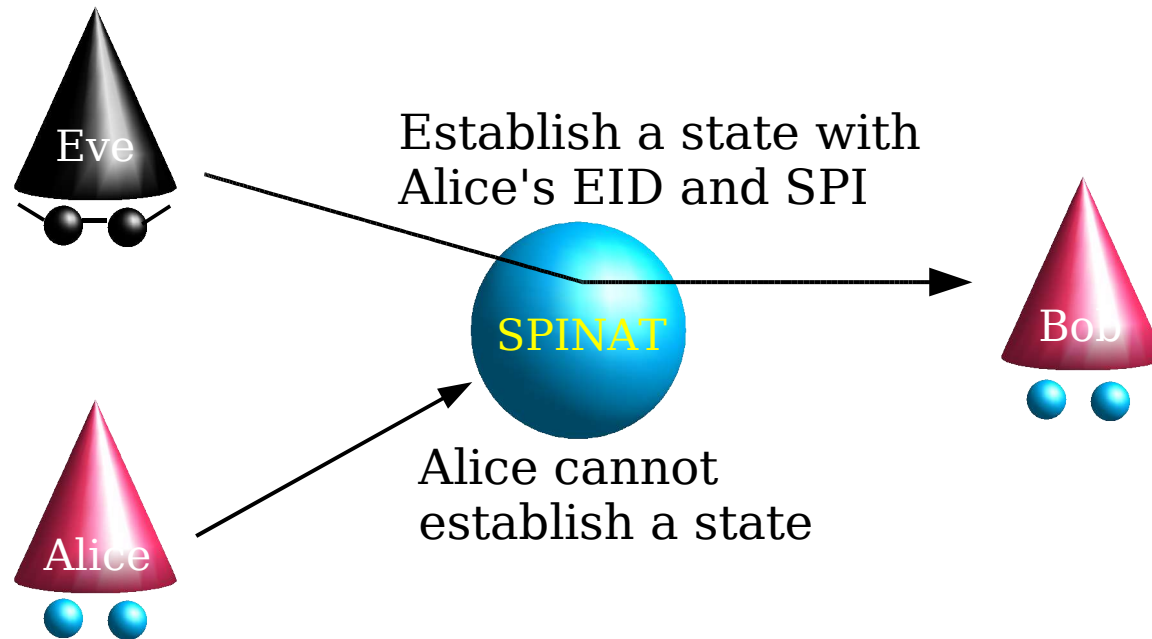
Asymmetric communication path



Security Considerations

- MitM may change SPIs on the fly
- SPI is only an index to an IPSec SA
- The actual security is based on the shared session keys

Running ahead attack



Solution: EIDs must be random during each negotiation (Use BLIND with key-exchange and mobility signaling).

Public key verification

- ✓ Identity protection hides public keys.
- ✓ Solution: Separate registration protocol with anonymous keys
- ✓ Public key verification may DoS problems in busy servers.
- ✓ Solution: Anonymous authentication with hash chains and secret splitting (Ylitalo ISC'04)

Conclusions

- ✓ Our SPINAT solution is based on observation that overlay routers implement Network Address Translation functionality.
- ✓ The presented changes do not change the existing security level of IPSec.
- ✓ SPINAT does not require UDP tunneling and supports asymmetric routing.
- ✓ SPINAT functionality can be integrated to middle-boxes in any overlay routing architecture (e.g. In i3 nodes)

Thank You!

Any questions?