

# IPSEC

## Modes of Operation

# IPSEC

- ❑ To establish a secure IPSEC connection two nodes must execute a key agreement protocol.
  - ❖ The sub-protocol of IPSEC that handles key negotiations is called IKE (Internet Key Exchange).
- ❑ First, assume two nodes have agreed on keys (via IKE) and see how they proceed to protect their communication via IPSEC.

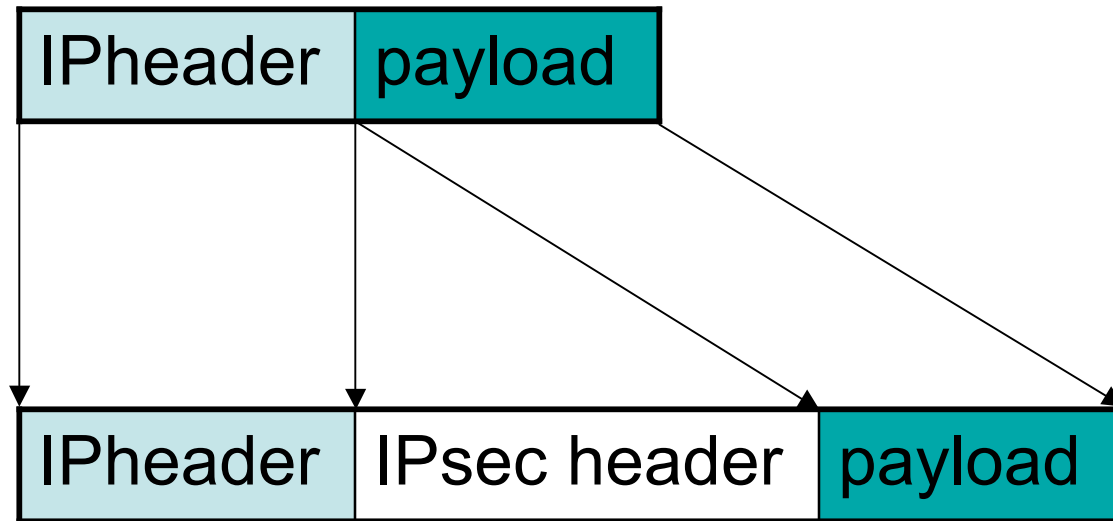
# Security Associations

- An IPsec protected connection is called a security association.
  - ❖ IPsec is a level-3 protocol (runs on top of IP), and below TCP/UDP
  - ❖ Security associations may either be end-to-end or link-to-link.
- Two modes of encapsulating IPsec data into an IP packet define two modes of operation:
  - ❖ Transport mode and tunnel mode.

# Security Parameter Index (SPI)

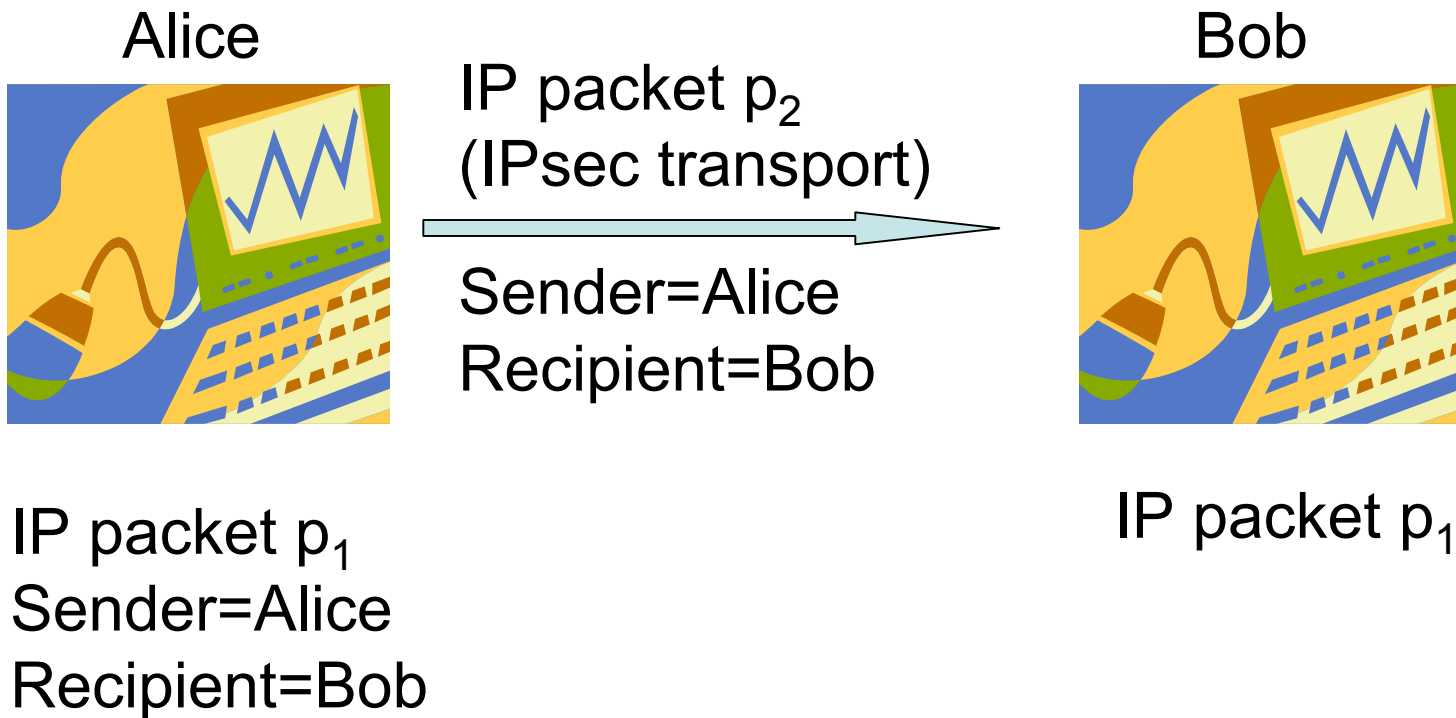
- The IPsec protocol maintains two databases:
  - ❖ Security association database. Indexed by SPI's, contains the information needed to encapsulate packets for one association: cryptographic algorithms, keys, sequence numbers, etc.
  - ❖ Security policy database: Allows for implementation of packet filtering policies. Defines whether or not to accept non-protected packets, what to require, etc.

# Transport mode

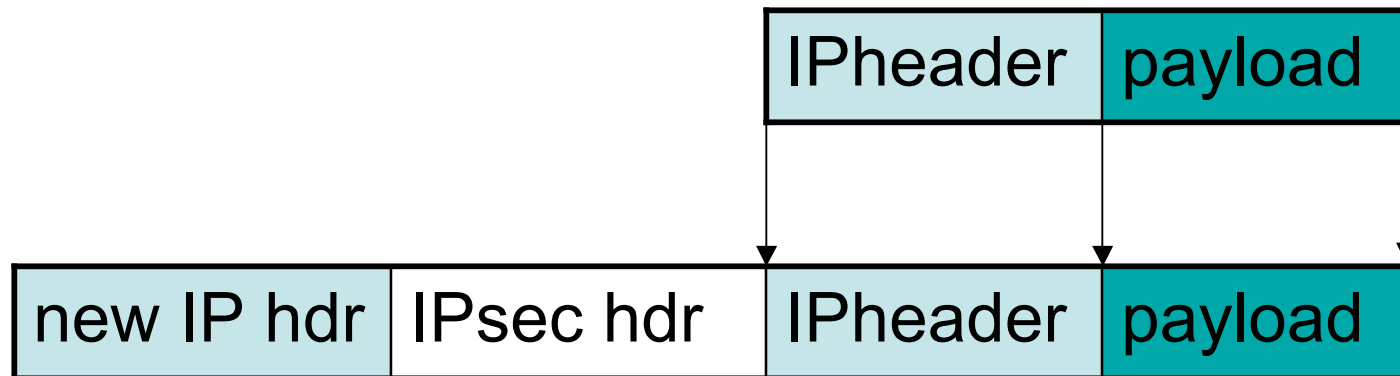


Transport mode was designed to save bandwidth in end-to-end associations. The payload is typically encrypted and authenticated. The IPheader is in the clear, and may or may not be authenticated.

# Transporting

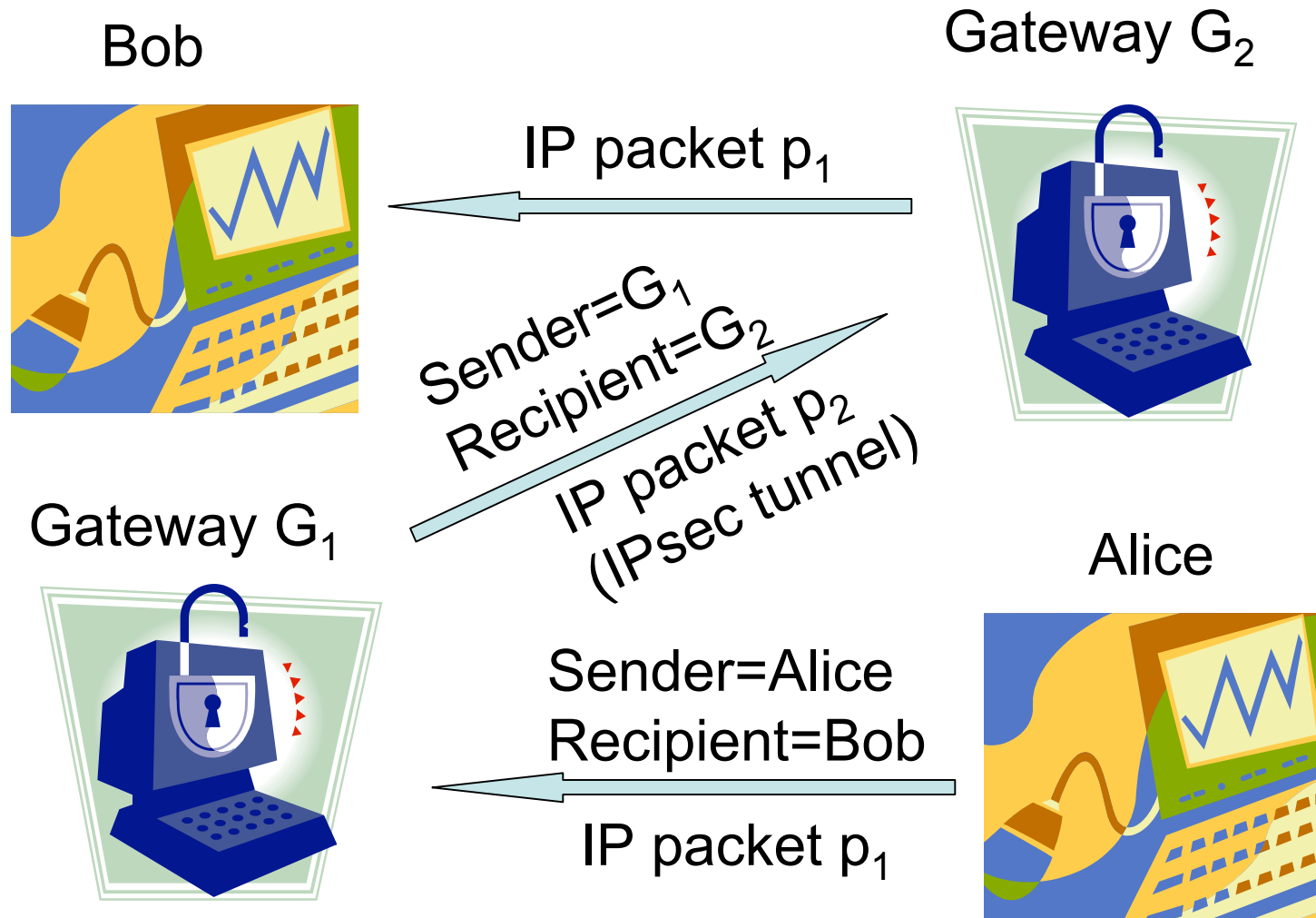


# Tunnel Mode



Tunnel mode protects both the payload and IP header of the original packet. If encryption is used between gateways in tunnel mode, then it reduces information for traffic analysis.

# Tunneling



# Adding IPSec to IPv4

version: 4bits
header length: 4bits (unit = 4-octet)
type of service: 1 octet
packet length: 2 octets
packet identification: 2 octets
flags: 3 bits
fragment offset: 13 bits
hops remaining (TTL): 1 octet
protocol: 1 octet
header checksum: 2 octets
source address: 4 octets
destination address: 4 octets
options: variable

Regular IP protocol values:  
TCP=6; UDP=17; IP= 4

IPsec protocol values:  
ESP=50 and AH=51

The communication  
protocols are specified  
in the IPsec header

# Adding IPsec to IPv6

version  type of service   flow label: 4 octets
payload length: 2 octets
next header: 1 octet (specifies protocol)
TTL: 1 octet
source address: 16 octets
destination address: 16 octets

# Authentication Header (AH)

next hdr: 1 octet (communication protocol)
payload length: (AH header length): 1 octet
unused: 2 octets
SPI (Security Parameter Index): 4 octets
sequence number: 4 octets
authentication data: variable

The Authentication Header authenticates data -- the protocol field is unencrypted, so it is available for firewall rule-based decisions. AH authenticates not only the IP payload but all “immutable” IP header components, such as source and destination addresses. This creates incompatibilities with NAT boxes in end-to-end associations.

# ESP (Encapsulating Security Payload)

- ❑ ESP allows for encryption, as well as authentication.
  - ❖ Both are optional, defined by the SPI and policies.
  
- ❑ ESP does not protect the IP header, only the payload
  - ❖ But, in tunnel mode everything is encapsulated
  
- ❑ If ESP encryption is enabled, then everything after the ESP header is encrypted
  - ❖ Communication protocol, ports (NATs and firewalls need this information).

# ESP encapsulation

SPI (Security parameter Index): 4 octets
sequence number: 4 octets
IV (initialization vector): variable
data: variable
padding: variable
padding length: 1 octet (unit length: octets)
next header/protocol type
authentication data

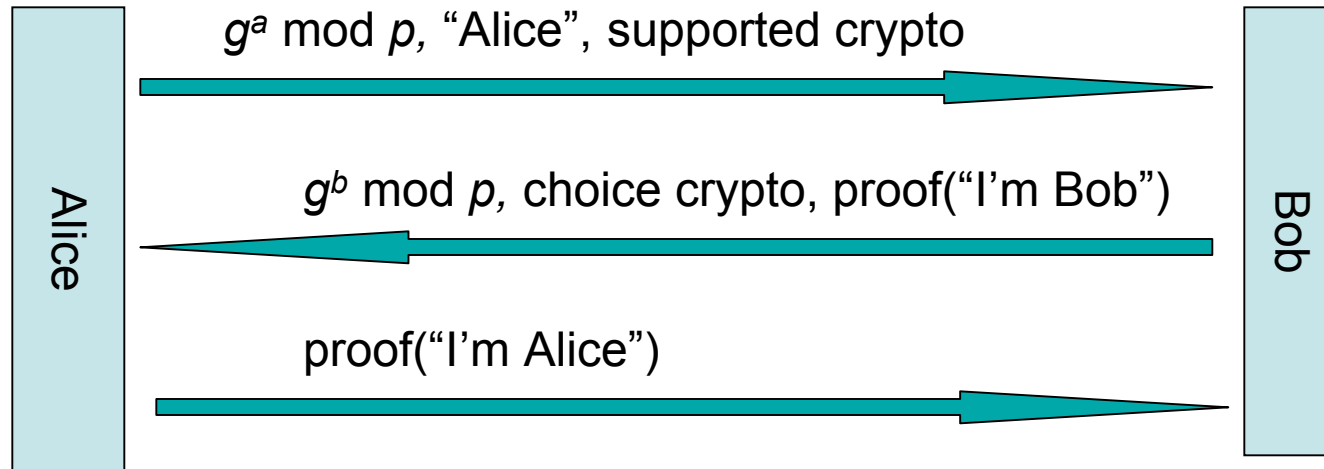
IKE

Internet Key Exchange

# IKE Phases

- In a design similar to Kerberos, IKE performs a phase 1 mutual authentication based on public keys and phase 2 re-authentication based on shared secrets (from phase 1).
  - ❖ This allows multiple SAs to re-use the same handshake.
- Phase 1 has two modes:
  - ❖ Aggressive mode (3 messages)
  - ❖ Main mode (6 messages)

# IKE Phase 1: Aggress. Mode



In aggressive mode, Alice chooses some Elgamal context  $(p, g)$ . Bob may not support it, and reject the connection. If that happens, Alice should try and connect to Bob using main mode.

Aggressive mode provides mutual authentication, and a shared secret  $g^{ab} \bmod p$ , which can be used to derive keys for the symmetric crypto protocols.

# IKE Phase 1: Main Mode

