DRONACHARYA
College of Engineering

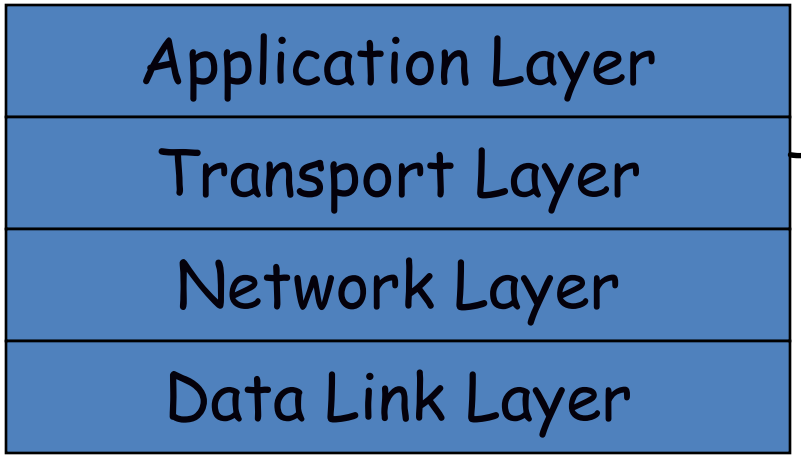
Computer Science & Engineering

Data Communication and Computer Networks

(MTCSE-101-A)

IPSec—An Overview

Security at What Level?



PGP, Kerberos,etc.

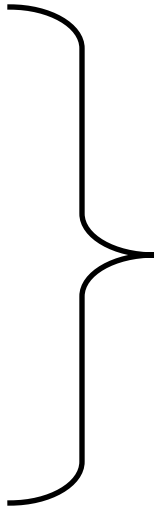
Transport Layer Security (TLS)

IP Security

Hardware encryption

Security Issues in IP

- source spoofing
- replay packets
- no data integrity or confidentiality



Fundamental Issue:
Networks are not (and will never be) fully secure

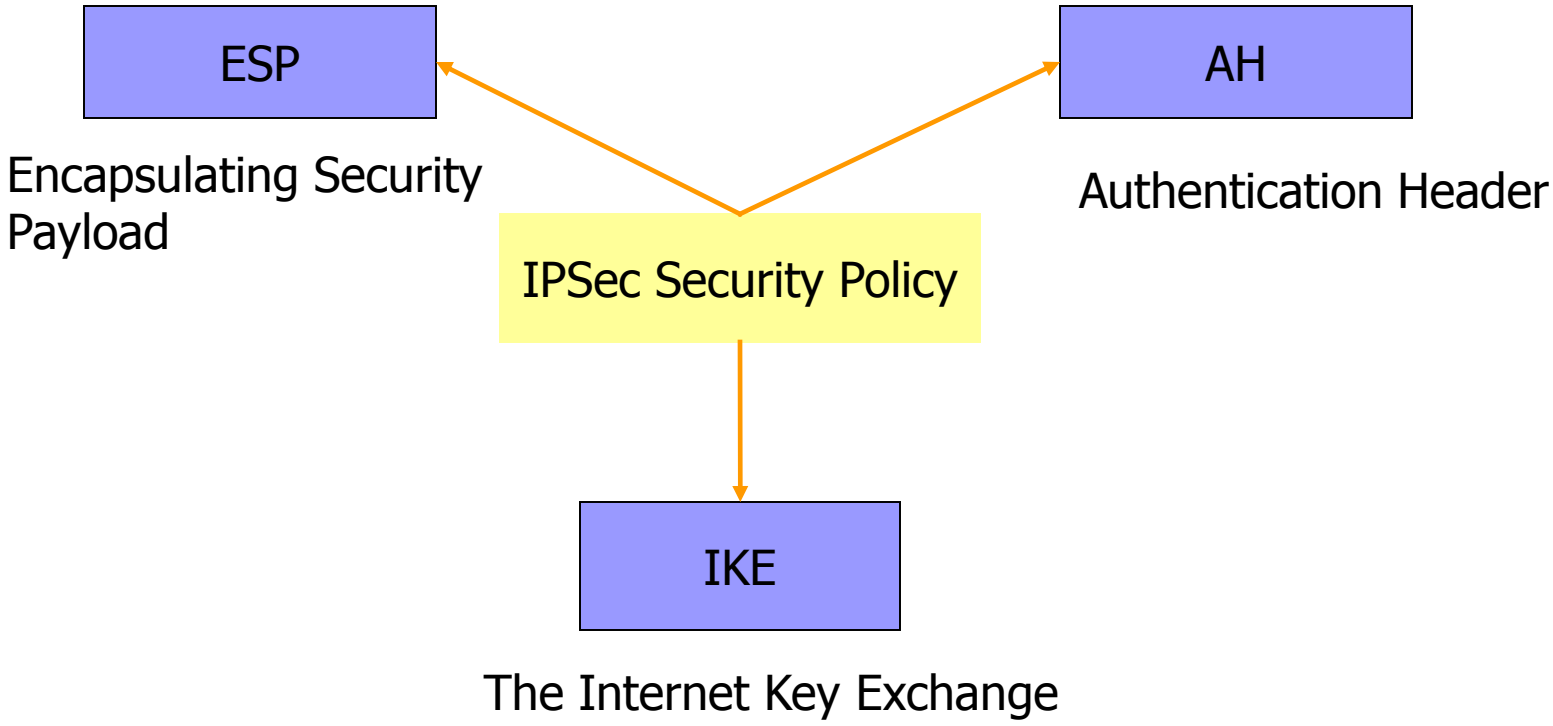
Goals of IPSec

- to verify sources of IP packets
  - *authentication*
- to prevent replaying of old packets
- to protect integrity and/or confidentiality of packets
  - *data Integrity/Data Encryption*

Outline

- Why IPsec?
- IPSec Architecture
- Internet Key Exchange (IKE)
- IPsec Policy
- Discussion

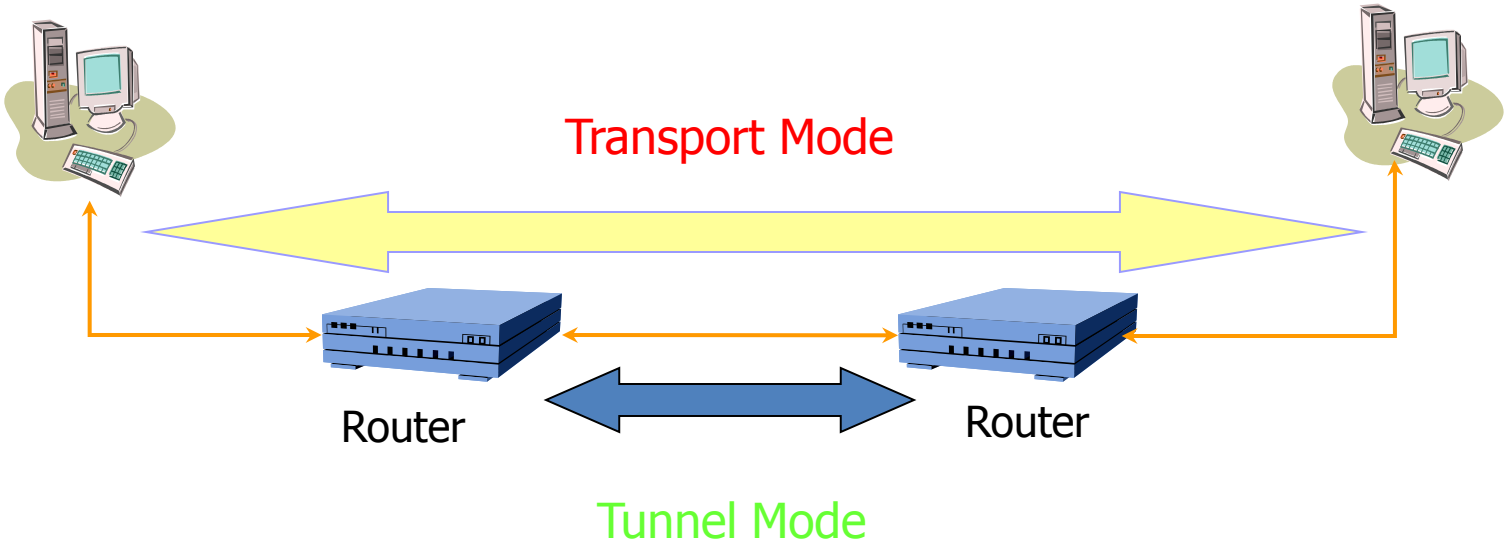
IPSec Architecture



IPSec Architecture

- IPSec provides security in three situations:
  - Host-to-host, host-to-gateway and gateway-to-gateway
- IPSec operates in two modes:
  - *Transport mode* (for end-to-end)
  - *Tunnel mode* (for VPN)

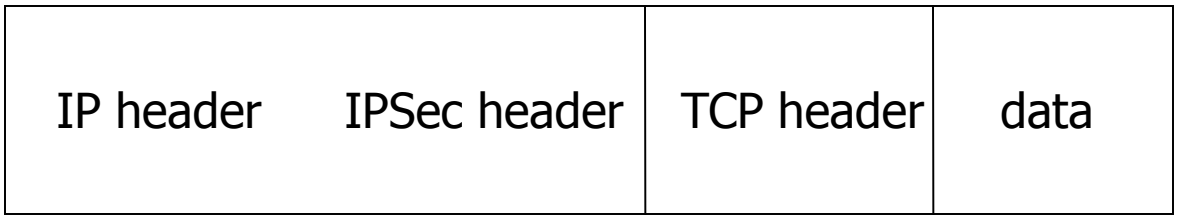
IPsec Architecture



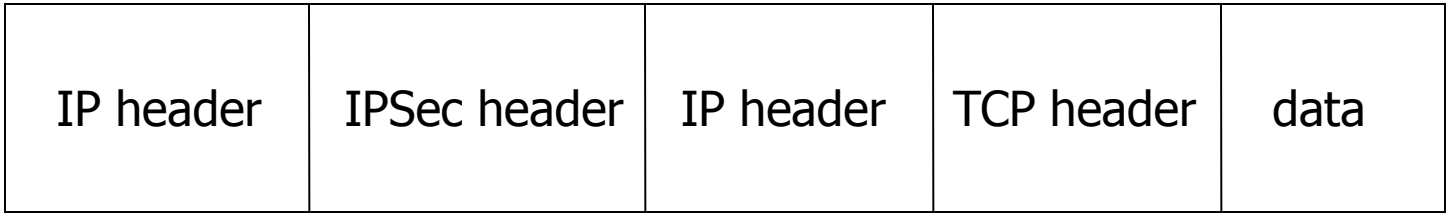
Various Packets

Original IP header TCP header data

Transport mode



Tunnel mode



IPSec

- A collection of protocols
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
  - Internet Key Exchange (IKE)
  - IP Payload Compression (IPcomp)

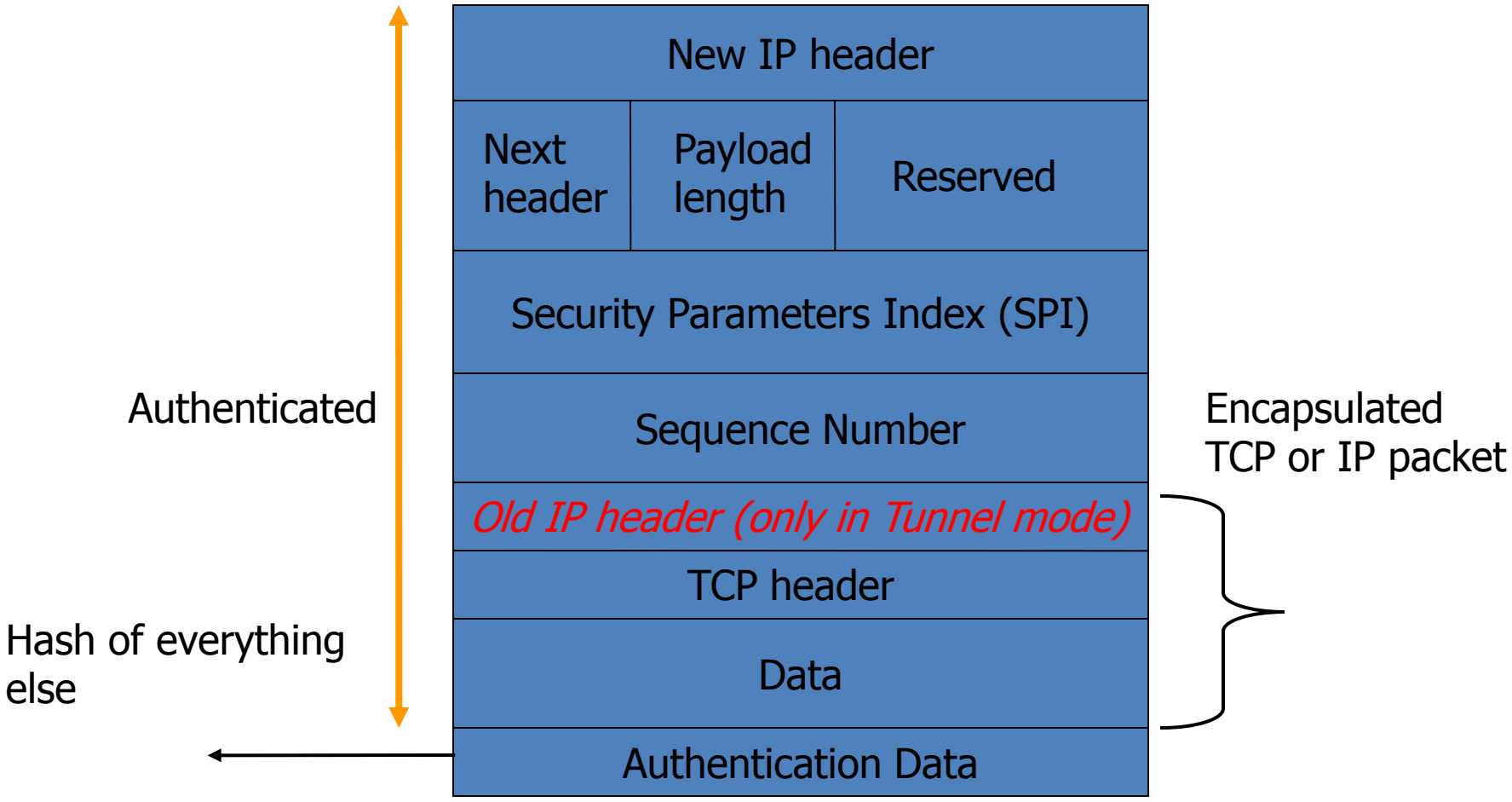
Authentication Header (AH)

- Provides source authentication
  - Protects against source spoofing
- Provides data integrity
- Protects against replay attacks
  - Use monotonically increasing sequence numbers
  - Protects against denial of service attacks
- NO protection for confidentiality!

AH Details

- Use 32-bit monotonically increasing sequence number to avoid replay attacks
- Use cryptographically strong hash algorithms to protect data integrity (96-bit)
  - Use symmetric key cryptography
  - HMAC-SHA-96, HMAC-MD5-96

AH Packet Details



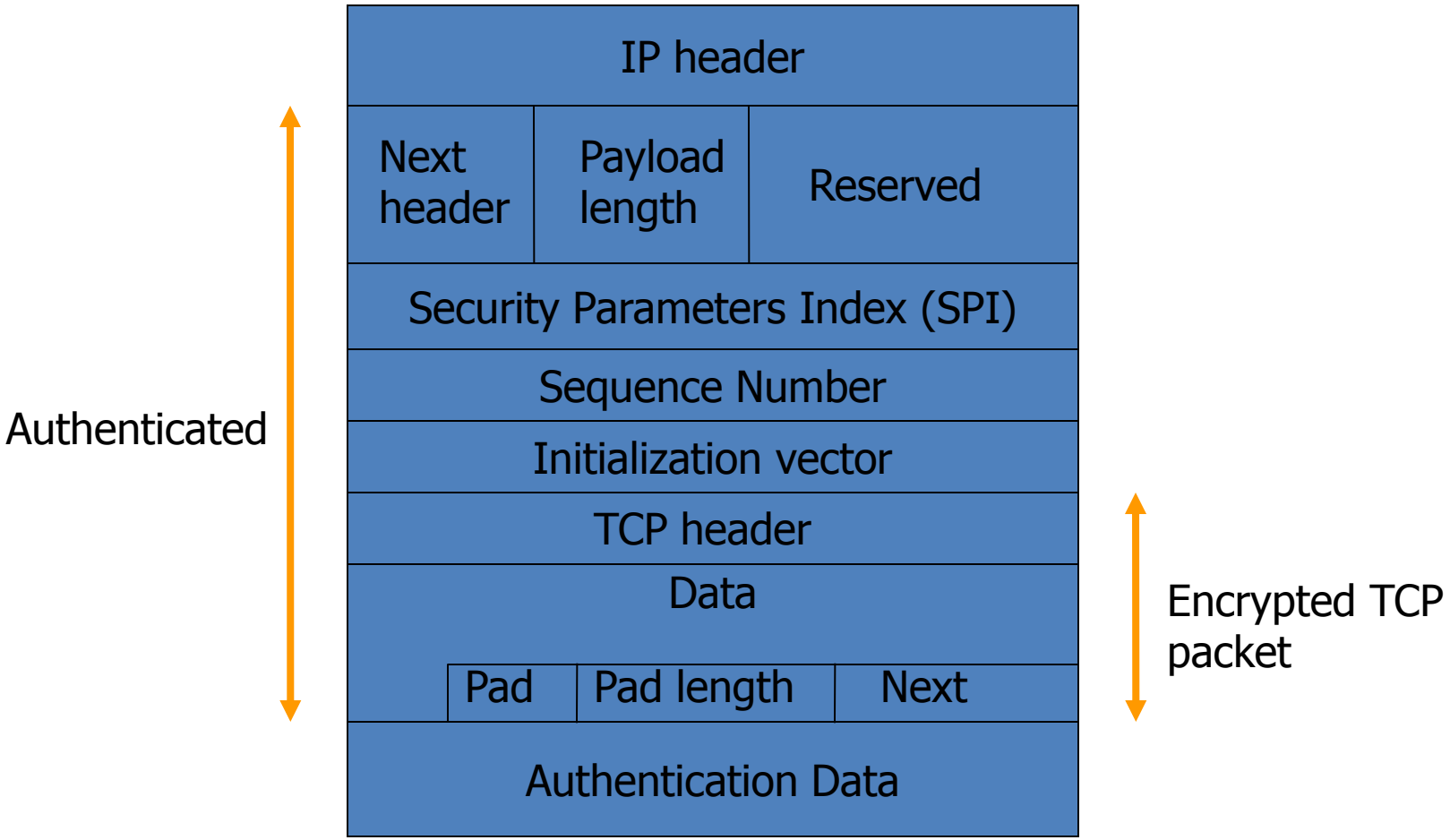
Encapsulating Security Payload (ESP)

- Provides all that AH offers, and
- in addition provides data confidentiality
  - Uses symmetric key encryption

ESP Details

- Same as AH:
  - Use 32-bit sequence number to counter replaying attacks
  - Use integrity check algorithms
- Only in ESP:
  - Data confidentiality:
    - Uses symmetric key encryption algorithms to encrypt packets

ESP Packet Details



Question?

1. Why have both AH and ESP?
2. Both AH and ESP use symmetric key based algorithms
   - Why not public-key cryptography?
   - How are the keys being exchanged?
   - What algorithms should we use?
   - Similar to deciding on the ciphersuite in SSL