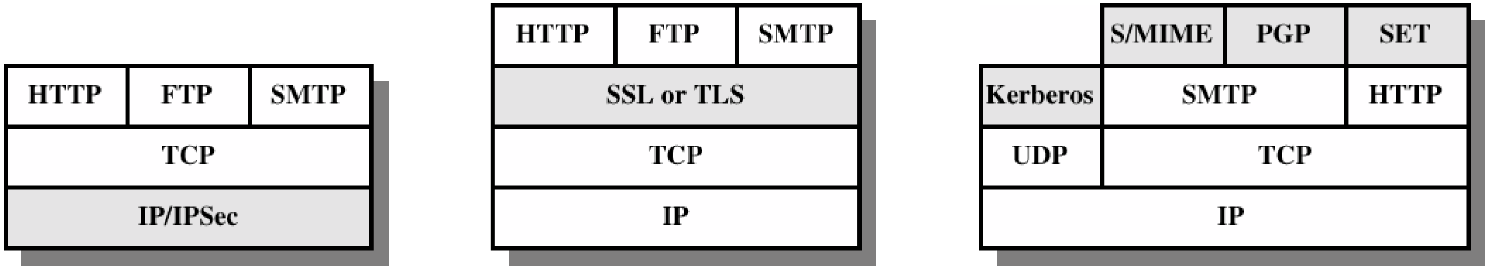
# IP Security

# Overview

- In 1994, Internet Architecture Board (IAB) issued a report titled "Security in the Internet Architecture".
- This report identified key areas for security mechanisms.
- Report emphasis on the need to secure the network infrastructure from unauthorized monitoring.
- and control of network traffic.
- And the need to secure end-user-to-end-user traffic using authentication and encryption mechanisms.
- Thus IAB included authentication and encryption as necessary security features in the next generation IP, which has been issued as IPv6.

# Security facilities in the TCP/IP protocol stack



HTTP | FTP | SMTP
TCP
IP/IPSec

HTTP | FTP | SMTP
SSL or TLS
TCP
IP

S/MIME | PGP | SET
Kerberos | SMTP | HTTP
UDP | TCP
IP

(a) Network Level

(b) Transport Level

(c) Application Level

# Definition

- **IPSec provides** a standard set of cryptographic algorithms that provides secure, trusted connections over TCP/IP and protects and filters the contents of IP packets at layer 3 (Network layer) of the OSI model.

**IPSec encrypted packets are resistant to:**

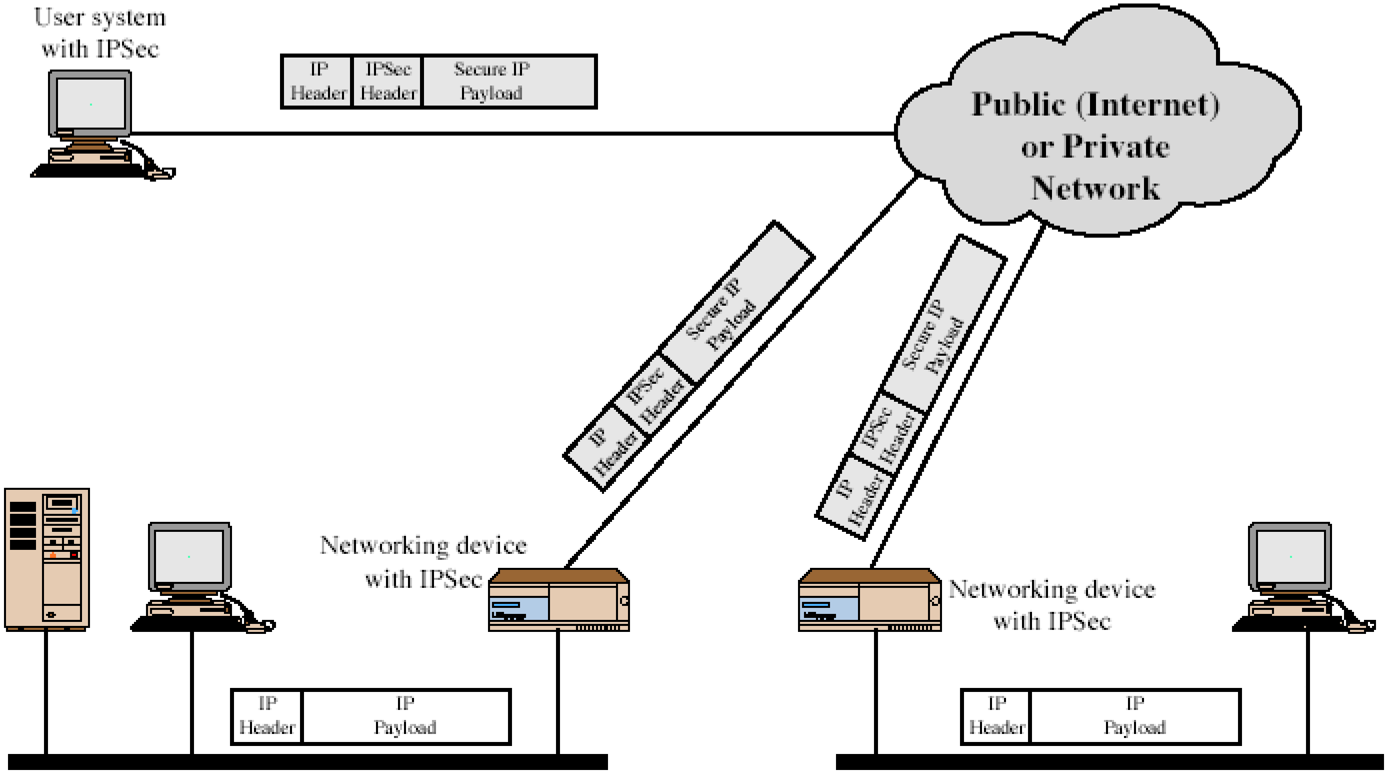
- IP Spoofing
- Man-in-the-middle attack
- DOS Attacks
- Eveasedropping/packet sniffing
- Payload/data modification

# Applications of IPSec

- Secure branch office connectivity over the internet e.g.VPN over the internet.
- Secure remote accessover the internet.
- Establishing extranet and intranet connectivity with partners.
- Enhancing electronic commerce security.

IPSec can encrypt and/or authenticate traffic at IP level.Thus, all distributed applications (including remote logon, client/server, e-mail, file transfer, web access, and so on) can be secured.

# IPSec Usage


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

## Benefits of IPSec

- In a firewall/router provides strong security to all traffic crossing the perimeter
- Is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users if desired
- additionally in routing applications:
  - assure that router advertisments come from authorized routers
  - neighbor advertisments come from authorized routers
  - insure redirect messages come from the router to which initial packet was sent

# IPSec Services

- Two protocols are used to provide security:
  - Authentication Header Protocol (AH)
  - Encapsulation Security Payload (ESP)
- Services provided are:
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets
    - a form of partial sequence integrity
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

- To create a secure IPSec encrypted connection, both sides require a compataible (but not identical)IPSec policy.
- Compatibility is negotiated through ISAKMP.

Once ISAKMP ensures that both parties are involved in an IPSec connection meet a common and compatible set of requirements, a SA is assigned to them

- Like a sophisticated firewall, Ipsec can filter packets on the basis of source and destination address, and the no of ports

# Security Associations

- a one-way relationship between sender & receiver that affords security for traffic flow
- defined by 3 parameters:
  - Security Parameters Index (SPI)
    - a bit string
  - IP Destination Address
    - only unicast allowed
    - could be end user, firewall, router
  - Security Protocol Identifier
    - indicates if SA is AH or ESP
- has a number of other parameters
  - seq no, AH & EH info, lifetime etc
- have a database of Security Associations

# Security Association Database

- SAD normally has following parameters:
- **Security Parameter Index**
  - Bit value used to identify SA
- **Sequence Number Counter**
  - Bit value used to generate sequence numbers
- **Sequence Counter Overflow**
  - A flag whose value indicates that overflow of sequence numbers
- **Anti-Replay Window**
  - Indicates whether a packet is a replay
- **AH Information**
  - Authentication algorithms, keys
- **ESP Information**
  - Encryption and Authentication algorithms, keys, initialization values, key life time etc.
- **Lifetime of this Security Association**
  - Time interval or byte count after which SA must be replaced
- **IPSec Protocol Mode**
  - Tunnel or Transport or wildcard
- **Path MTU**
  - Path maximum transmission Unit of a Packet aging variables

# Security Policy Database

- The means by which IP traffic is related to specific SAs is SPD.
- Simply, SPD points to a subset of IP traffic and the associated SA to that traffic.
- In complex environment, there can be multiple entries for a SA.
- For any outbound packet, SPD does the following sequence of steps:
  - Compare the values for the appropriate fields in the packet, which will point to zero or more fields.
  - Determine the SA if any for this packet and its associated SPI.
  - Do the required IPSec processing (ESP or AH)

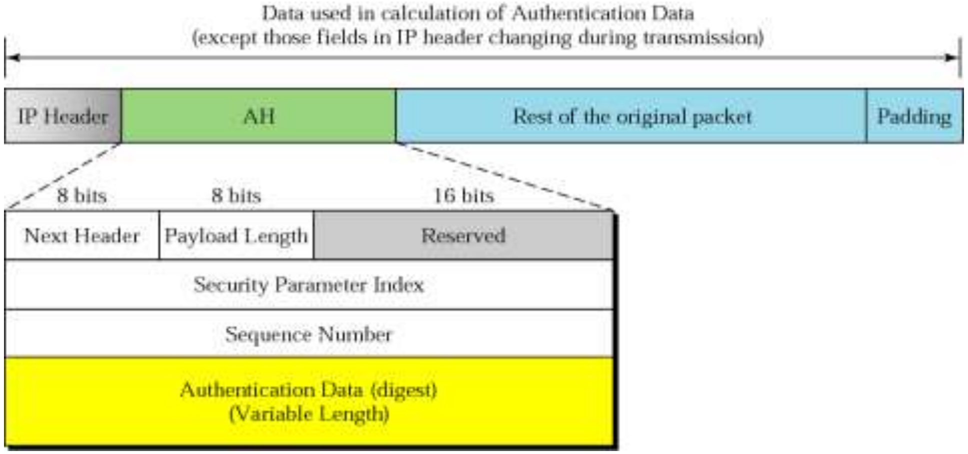
# Security Policy Database

- Each specific SPD entry is called Selector.
- The following selectors determine an SPD entry:
- Remote and Local IP Addresses
  - This may be a single IP address or range of addresses or wildcard(mask) address
- Next layer Protocol
  - TCP, UDP etc.
- Name
  - A user identifier from the operating system
- Local and Remote Ports
  - TCP or UDP port values

# AH

- Authentication Header (AH) protocol is designed to authenticate the source host and to ensure the integrity of the payload carried by the IP packet.
- The protocol calculates a message digest, using a hashing function and a symmetric key, and inserts the digest in the authentication header.
- The AH protocol provides source authentication and data integrity, but not privacy.

This is transport AH →

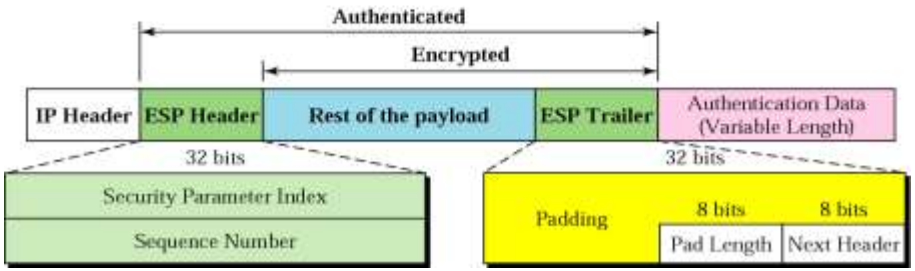

Data used in calculation of Authentication Data
(except those fields in IP header changing during transmission)
IP Header
AH
Rest of the original packet
Padding
8 bits
8 bits
16 bits
Next Header
Payload Length
Reserved
Security Parameter Index
Sequence Number
Authentication Data (digest)
(Variable Length)

- Steps for authentication header:
  - AH is added to the payload with the authentication data field set to zero.
  - Padding may be added to make the total length even for a particular hashing algorithm
  - Hashing is based on total packet. For message digest, only those fields of IP header that don’t change during transmission are considered.
  - Authentication data are included in the authentication header
- Payload length: Length of AH in 4-byte multiples.
- SPI: plays the role of VCI
- Sequence number: for anti replay

# ESP

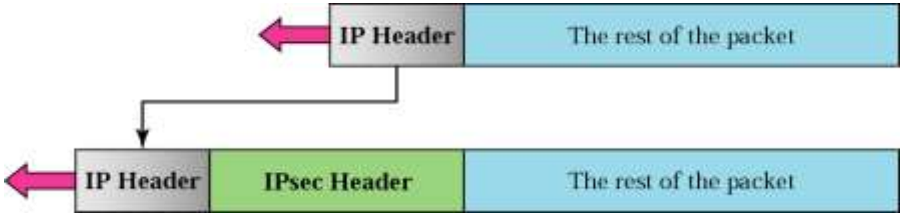
- Encapsulation Security Payload (ESP) provides source authentication, privacy and integrity.
- Steps
  - ESP trailer is added to the payload
  - Payload and trailer or encrypted
  - ESP header is added
  - ESP header, payload and ESP trailer are used to create authenticated data.
  - Authenticated data are added at the end of ESP trailer.

This is transport ESP →

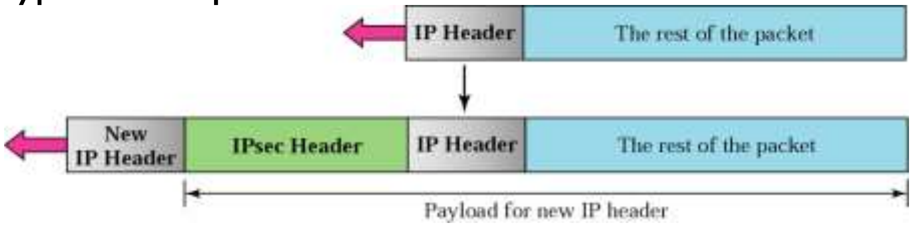


# Two Modes of Operation

- IPSec operates in two different modes. Mode defines where the IPSec header is applied to the IP packet.
  - Transport mode
    - IPSec header is added between the IP header and the rest of the packet.
    - Most logical when IPSec is used end-to-end



  - Tunnel mode
    - IPSec header is placed in front of the original IP header.
    - The IPSec header, the preserved IP header, and the rest of the packet are treated as the payload.
    - Can be used when IPSec is applied at intermediate point along path (e.g., VPN)
    - Results in slightly longer packet
    - Note that data may be encrypted multiple times


IP Header
The rest of the packet
New IP Header
IPsec Header
IP Header
The rest of the packet
Payload for new IP header