IP Security

Cunsheng Ding
HKUST, Kong Kong, China

Agenda

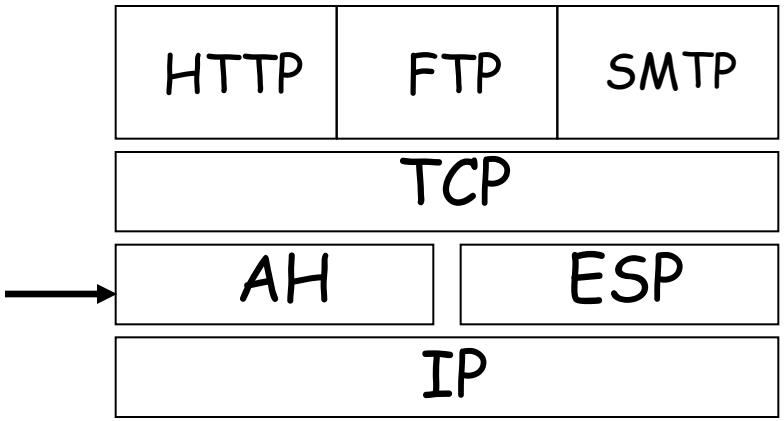
- Some attacks against the IP
- Brief introduction to IPSec
- Building Block: Security Association Database
- Building Block: Security Association Database
- Building Blocks: IPSec Protocols - ESP and AH
- Building Block: Security Policy Database
- Building blocks: Key Management Protocols
- The Whole Picture of IPSec

The Internet Layers

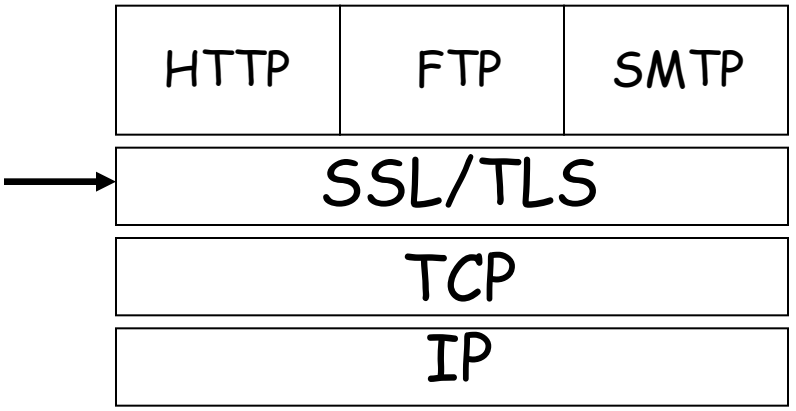
Application	telnet,ftp,http, smtp,set
Transport/session	TCP, UDP
Internet	IP
Interface	Network technology protocols

smtp = simple mail transfer protocol

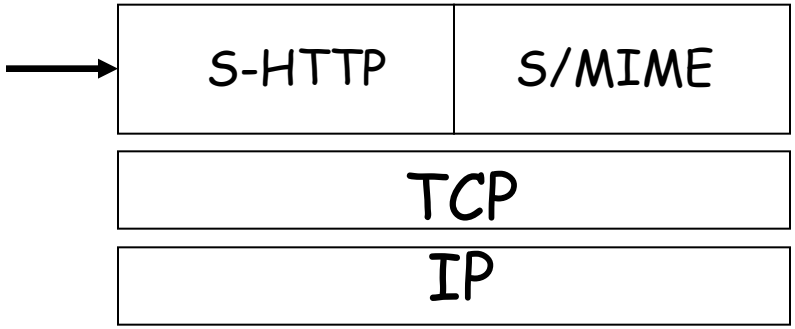
Where can we put security?



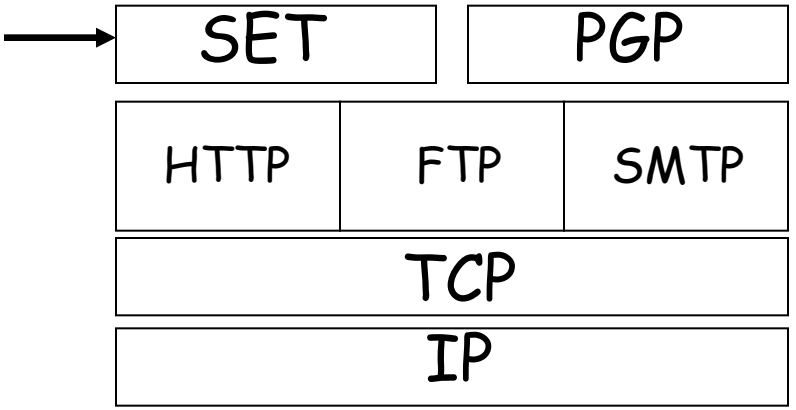
Network approach



Transport approach



Application approach



Presentation approach

Advantages and disadvantage of each?

Attacks Against IP

- A number of attacks against IP are possible.
  - Typically, these exploit the fact that IP does not perform a robust mechanism for sender authentication.
- IP Spoofing
  - This is where one host claims to have the IP address of another.
- IP Session Hijacking
  - It is an attack whereby a user's session is taken over, being in the control of the attacker.
  - If the user was in the middle of email, the attacker is looking at the email, and then can execute any commands he wishes as the attacked user.

Conclusion: Security mechanism at the network layer would help.

Brief Introduction to IPSec

Internet Engineering Task Force Standardization

- 1992: IPSEC WG (IETF)
  - Define security architecture
  - Standardize IP Security Protocol and Internet Key Management Protocol
- **1998: revised version of IPSec Architecture**
  - *IPsec protocols* (two sub-protocols AH & ESP)
  - *Internet Key Exchange* (IKE)
- 2005: IKEv2 (RFC4301-4306)
- 2014: Revised IKEv2, adopted as a standard

IPsec: Network Approach

- Provides security for IP and upper layer protocols
- Suit of algorithms:
  - Mandatory-to-implement
    - Assures interoperability
  - Easy to add new algorithms

IP Security Overview

IPSec provides the following:

- Data origin authentication
- Connectionless data integrity
- Data content confidentiality
- Anti-replay protection
- Limited traffic flow confidentiality

Building Blocks:
Security Association Database

Security Association

- It is a one-way relationship between a sender and a receiver.
- It associates security services and keys with the traffic to be protected.
- It is identified by:
  - Security Parameter Index (SPI) → retrieve correct SA parameters from Security Association Database (SAD)
  - IPSec protocol identifier (AH or ESP)
  - Destination address (firewall, router)

Security Association

- Defines *security services* and *mechanisms* between two end points (or IPsec modules):
  - Hosts
  - Network security gateways (e.g., routers, application gateways)
  - Hosts and security gateways
- Defines parameters, mode of operation, and initialization vector
  - e.g., Confidentiality using ESP with DES in CBC mode with IV initialization vector
- May use either Authentication Header (AH) or Encapsulating Security Payload (ESP).

Security Association

- **Host A Security Association:**

```
# ipsecadm new esp -spi 1000 -src HostA \
   -dst HostB -forcetunnel -enc 3des -auth sha1 \
   -key 7762d8707255d974168cbb1d274f8bed4cbd3364 \
   -authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

- **Host B Security Association:**

```
# ipsecadm new esp -spi 1001 -src HostB \
   -dst HostA -forcetunnel -enc 3des -auth sha1 \
   -key 7762d8707255d974168cbb1d274f8bed4cbd3364 \
   -authkey 6a20367e21c66e5a40739db293cf2ef2a4e6659f
```

RemarK: src = source, dst = destination, keysize = 160 bits

spi is a binary string at most 32 bits, used to create and delete SA, the spi values between 0 and 100 are reserved.

SA -- Lifetime

- Amount of traffic protected by a key and time frame the same key is used
  - Manual creation: no lifetime
  - Dynamic creation: may have a lifetime

Building Blocks:
Security Policy Database

Security Policy Database (SPD)

- Defines:
  - What traffic to be protected
  - How to protect
  - With whom the protection is shared
- For each packet entering or leaving an IPsec implementation, SPD is used to determine security mechanism to be applied
- Actions:
  - Discard: do not let packet in or out
  - Bypass: do not apply or expect security services
  - Protect: apply/expect security services on packets

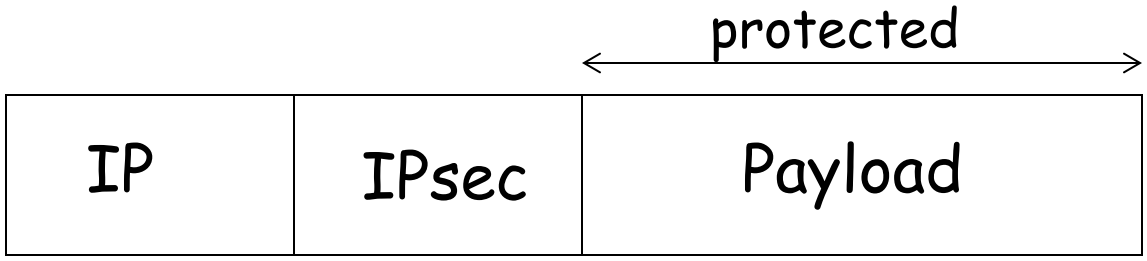
Building Blocks:
IPSec Protocols

IPSec Protocols

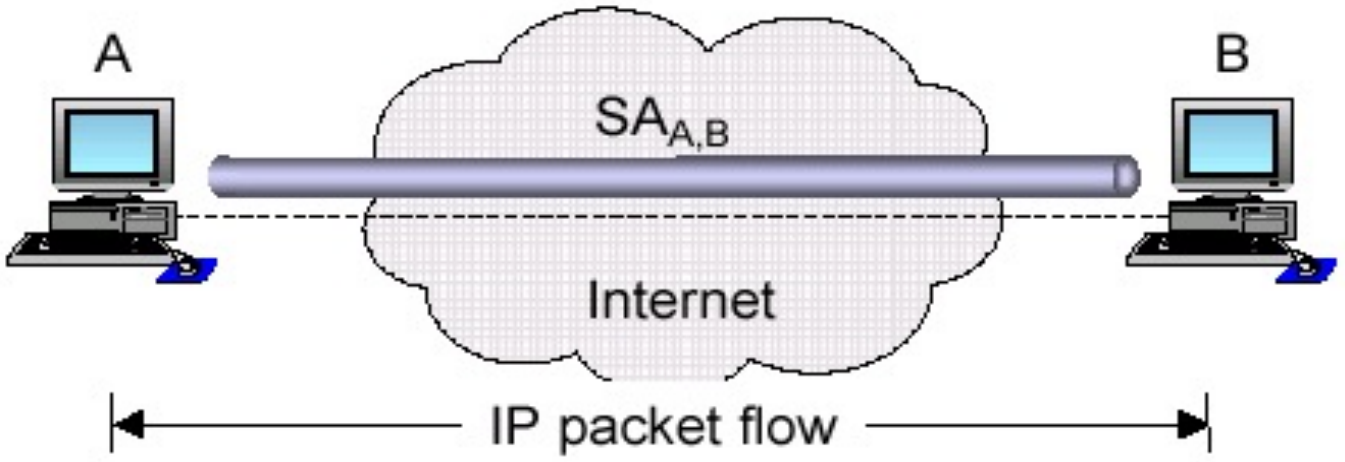
- *Encapsulating Security Payload (ESP)*
  - Proof of data origin, data integrity, anti-replay protection
  - Data confidentiality and limited traffic flow confidentiality
- *Authentication Header (AH)*
  - Proof of data origin, data integrity, anti-replay protection
  - No data confidentiality
  - May provide non-repudiation & anti-replay (it depends on the algorithm used.)

Transport Mode: AH & ESP

- Usage: protect upper layer protocols
  - IPSec header is inserted between the IP header and the upper-layer protocol header
  - Communication endpoints must be cryptographic endpoints (for end-to-end authentication), i.e., the endpoints generate/process IP header (AH, ESP).
  - Only data is protected.



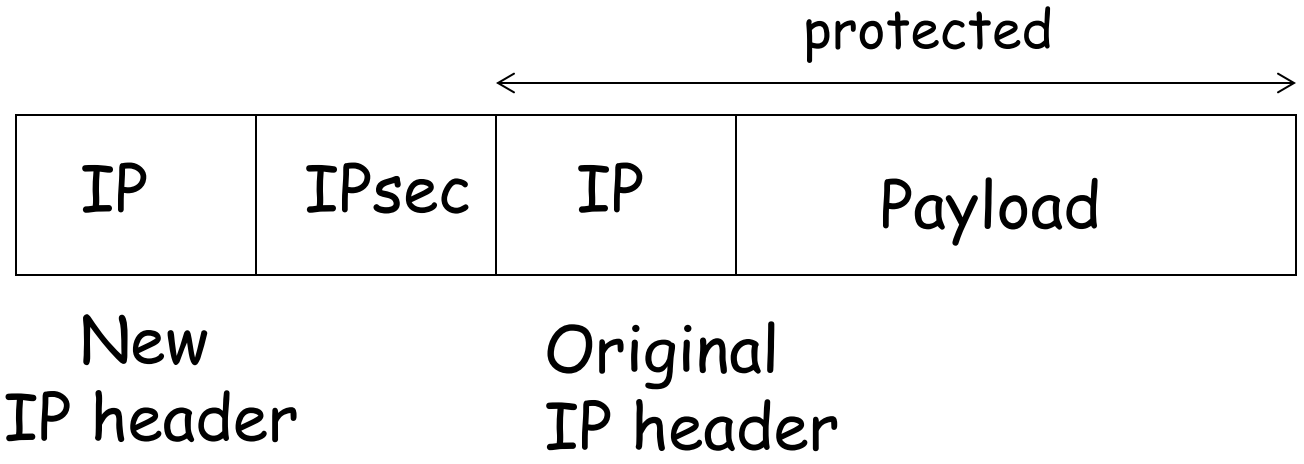
When is Transport Mode Used



Both endpoints are cryptographic endpoints, i.e. they generate / process an IPSec header (AH or ESP)

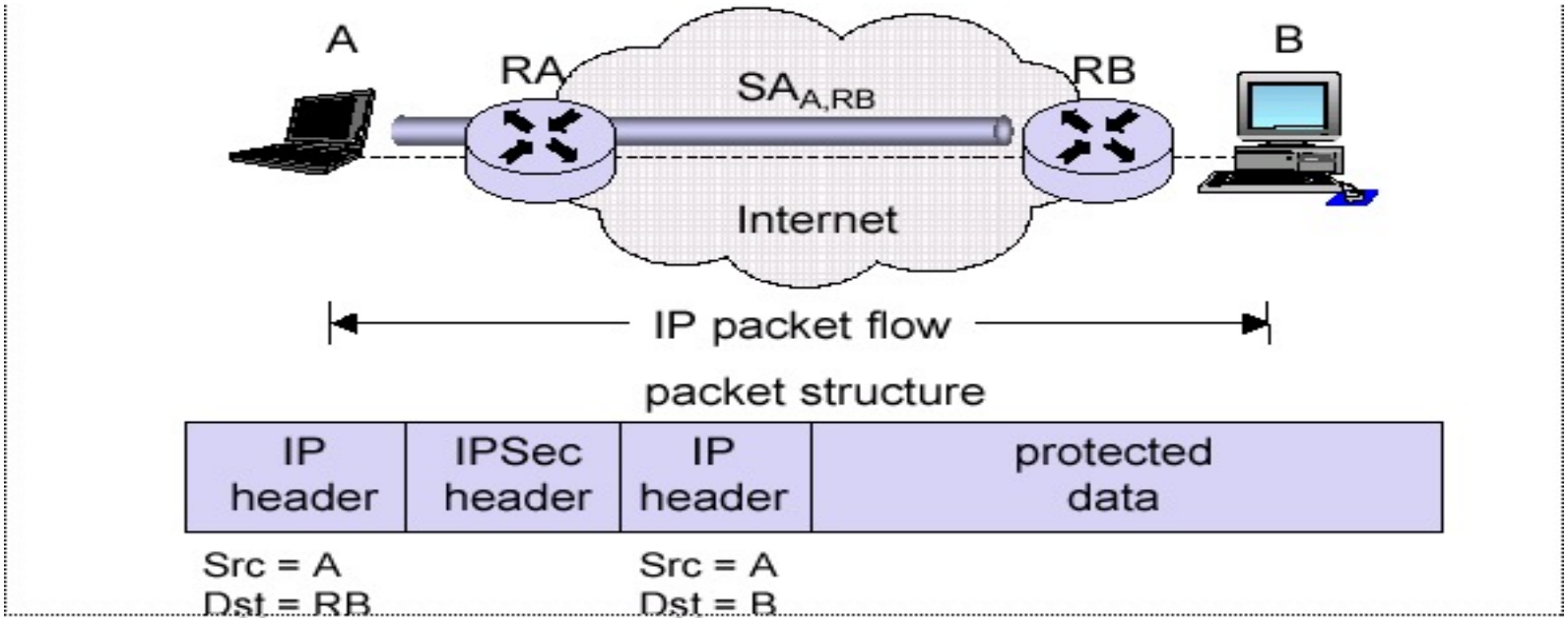
Tunnel Mode: AH & ESP

- **Usage:** protect entire IP datagram
  - Entire IP packet to be protected is encapsulated in another IP datagram and an IPsec header is inserted between the outer and inner IP headers



When Is Tunnel Mode Used

Tunnel mode is used when at least one cryptographic endpoint is not a communication endpoint of the secured IP packets.



Outer IP Header – Destination for the router.

Inner IP Header – Ultimate Destination

Encryption and Authentication Algorithms

- Encryption:
  - Triple DES in CBC mode (MUST)
  - AES in CBC mode (SHOULD+)
  - AES in CTR (counter) mode (SHOULD)
- Authentication:
  - HMAC-MD5-96 (MAY)
    - 96 truncated bits from 128 bits
  - HMAC-SHA-1-96 (MUST)
    - 96 truncated bits from 160 bits
  - AES-XCBC-96 (SHOULD+)
    - 96 truncated bits from 128 bits

Building Blocks:
Key management protocol
IKE

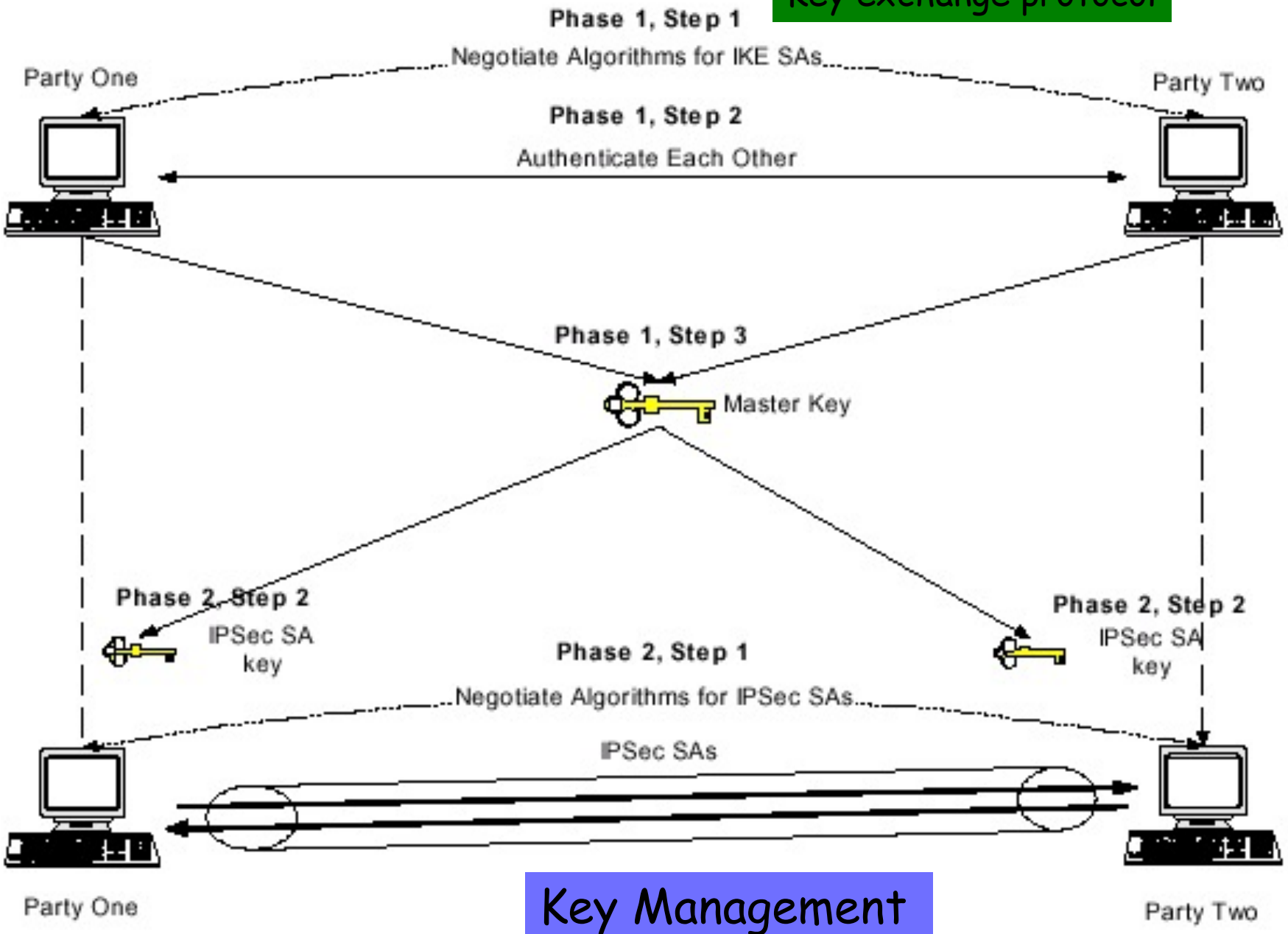
Key Management

- IPSec needs secret keys:
  - for transmitting and receiving both AH and ESP
- It supports two types of key management:
  - **Manual**: A system administrator manually configures each system with its own keys and with the keys of other communicating systems.
  - **Automated**: An automated system enable the on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system with an evolving configuration.

Key Management Protocol

- The management protocol is called "Internet Key Exchange (IKE)".
- It has two versions.
  - IKE 1998, IKEv2 2005, revised IKEv2 2014
- It is the most complicated sub-protocol of IPSec.
- Details of IKE 1998 are omitted in this course, but we will present its outline here.
- IKEv2: https://tools.ietf.org/html/rfc7296

Key exchange protocol



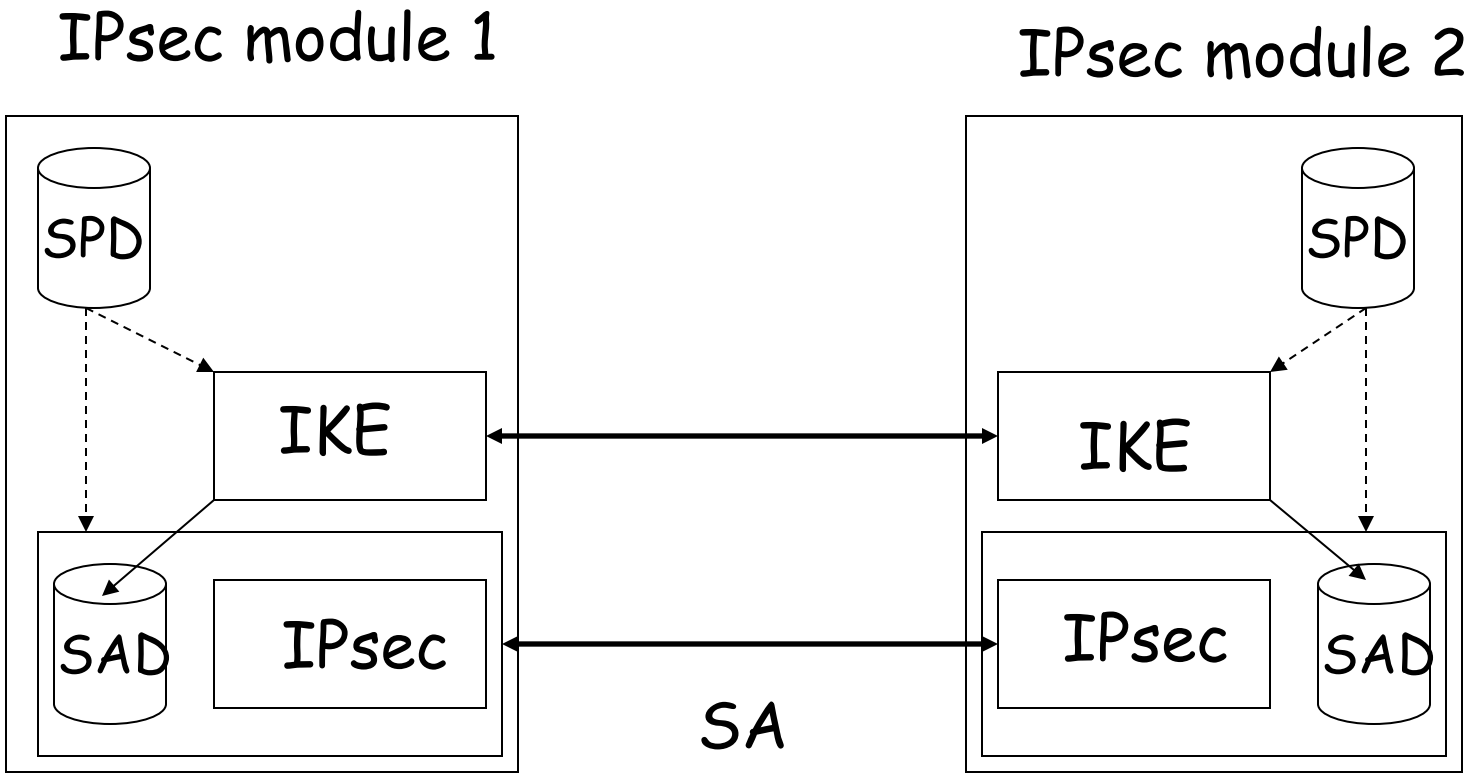
Key Management

Some entries in an IKE SA

- A mutual authentication method, which is one of:
  - A protocol based on a pre-shared secret key
  - A challenge-response protocol based on a public-key cipher
- A key-establishment method, which is one of:
  - The digital envelop protocol
  - The Diffie-Hellman key exchange protocol
- A cipher and a hash function
- Encryption and authentication keys

Whole Picture of IPSec

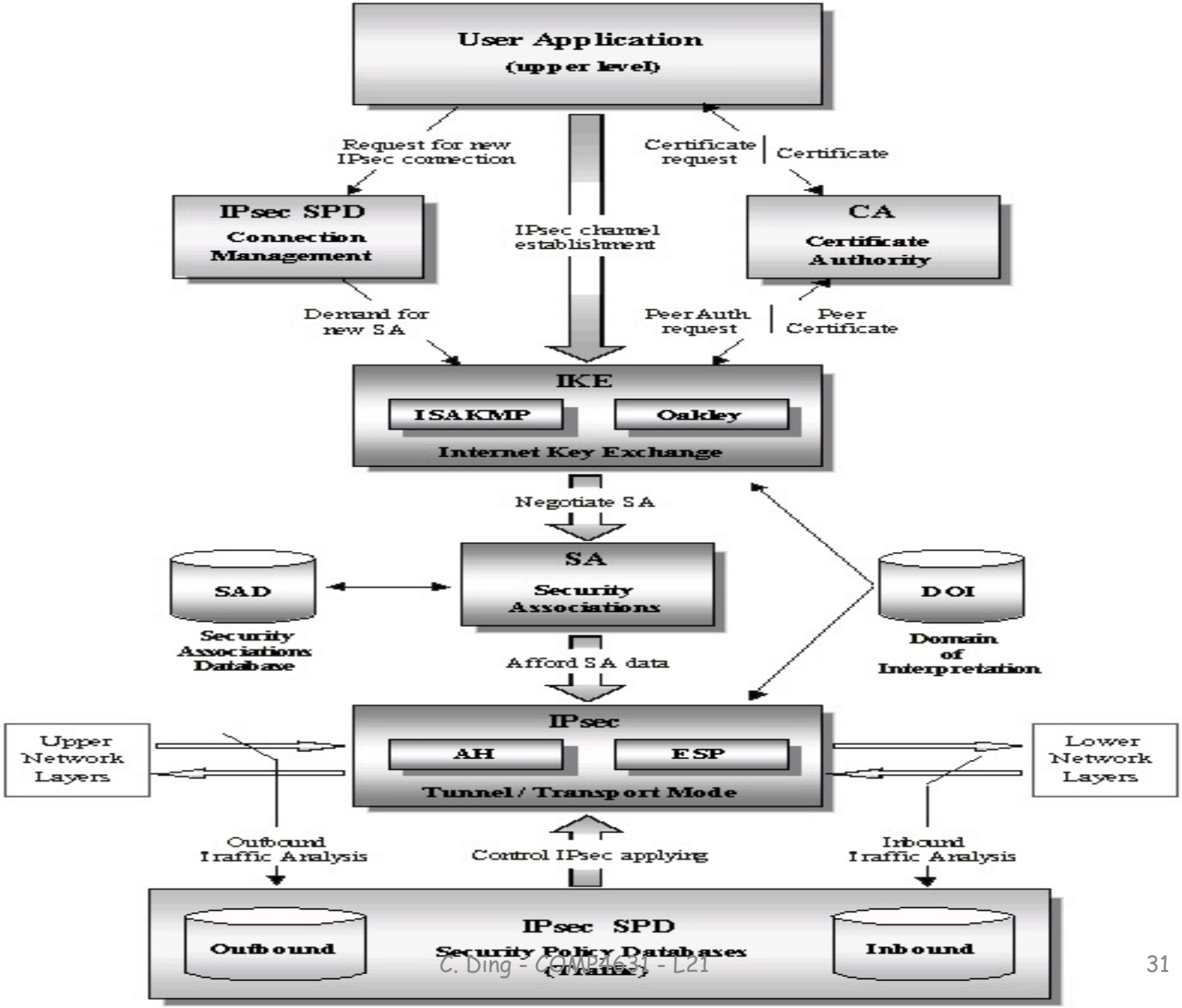
IP Security Architecture



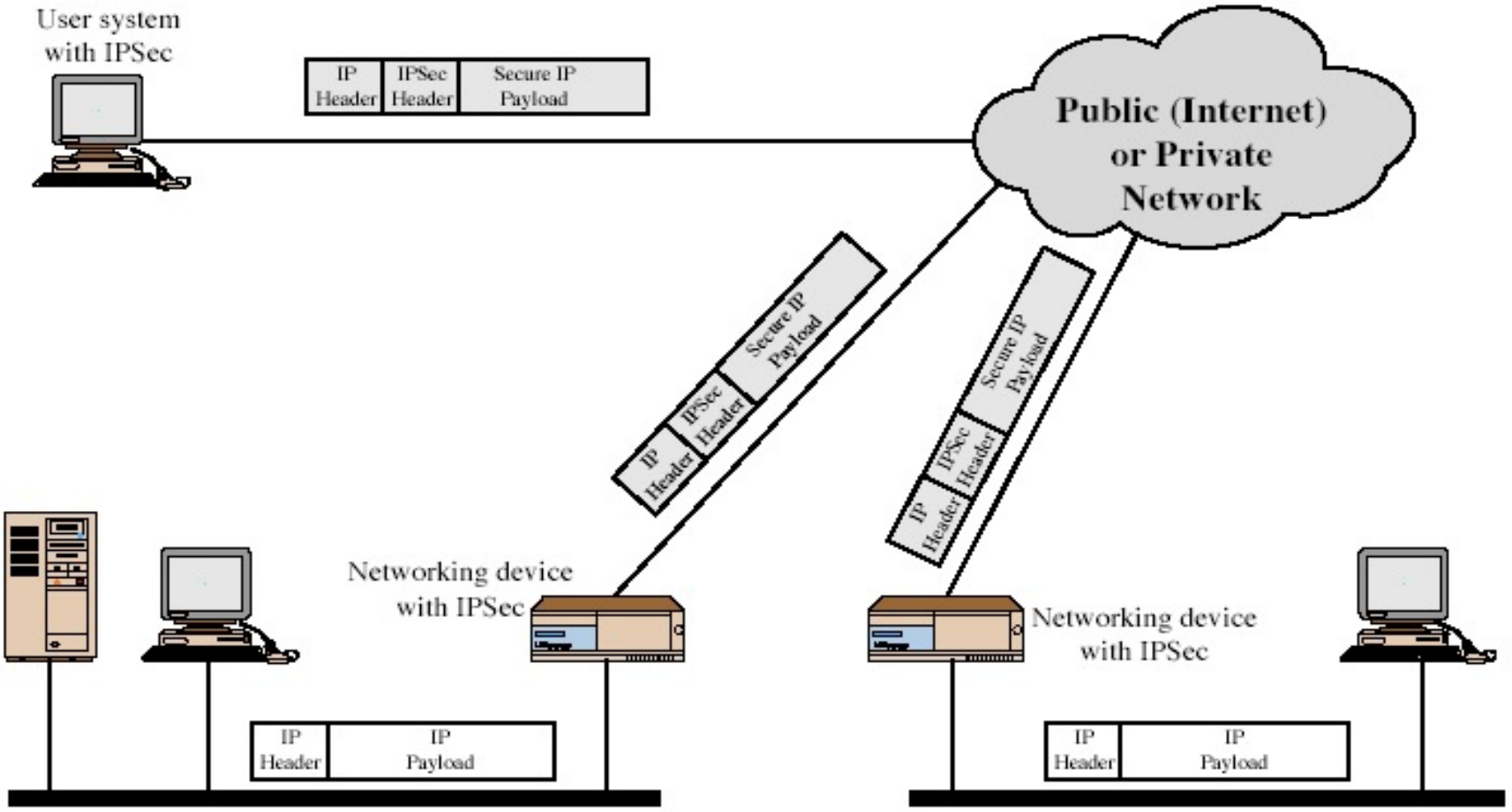
SAD: Security Association Database

SPD: Security Policy Database

IKE: Internet Key Exchange


User Application
(upper level)
Request for new IPsec connection
Certificate request
Certificate
IPsec SPD
Connection Management
IPsec channel establishment
CA
Certificate Authority
Demand for new SA
PeerAuth. request
Peer Certificate
IKE
ISAKMP
Oakley
Internet Key Exchange
Negotiate SA
SAD
Security Associations Database
SA
Security Associations
DOI
Domain of Interpretation
Afford SA data
IPsec
AH
ESP
Tunnel / Transport Mode
Upper Network Layers
Lower Network Layers
Outbound Traffic Analysis
Control IPsec applying
Inbound Traffic Analysis
IPsec SPD
Security Policy Database
(Traffic)
Outbound
Inbound

IPSec Uses


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

Applications of IPSec

- Using IPSec all distributed applications can be secured,
  - Remote logon,
  - client/server,
  - e-mail,
  - file transfer,
  - Web access
  - etc.

Benefits of Using IPSec

- The benefits of IPSec include:
  - IPSec can be transparent to end users.
  - There is no need to train users on security mechanisms
  - IPSec can provide security for individual aplication
    - By configuration, IPSec is applied to only one specified application.