INTERNET PROTOCOL SECURITY *AN OVERVIEW OF IPSEC*

OUTLINE:

- What Security Problem?
- Understanding TCP/IP.
- Security at What Level?
- IP Security.
- IPSec Security Services.
- Modes of operation.
- IPSec Security Protocols.
- Outbound/Inbound IPSec Processing.
- Real World Deployment Examples.

WHAT SECURITY PROBLEM?

Today's Internet is primarily comprised of :

- Public
- Un-trusted
- Unreliable IP networks

Because of this inherent lack of security, the Internet is subject to various types of threats…

INTERNET THREATS

- Data integrity

  The contents of a packet can be accidentally or deliberately modified.

- Identity spoofing

  The origin of an IP packet can be forged.

- Anti-reply attacks

  Unauthorized data can be retransmitted.

- Loss of privacy

  The contents of a packet can be examined in transit.

UNDERSTANDING TCP/IP

OSI Reference Model

Application Layer	Application HTTP SMTP FTP DNS FTP SNMP NFS
Presentation Layer	
Session Layer	
Transport Layer	TCP, UDP
Network Layer	IP
Logical Link Layer	Device Driver
Physical Layer	Network Adapter

UNDERSTANDING TCP/IP

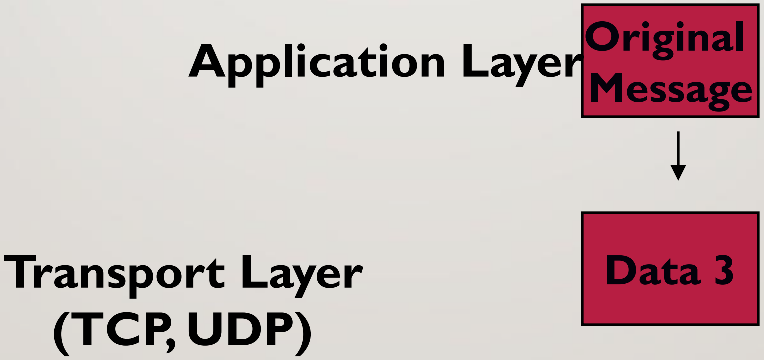
Encapsulation of Data for Network Delivery

Application Layer

Original Message

UNDERSTANDING TCP/IP

Encapsulation of Data for Network Delivery



Application Layer

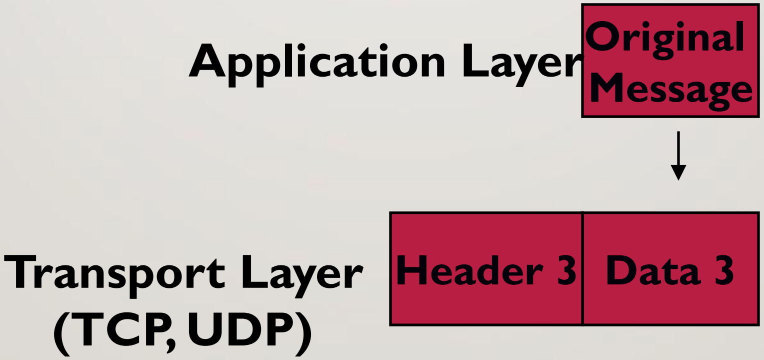
Original Message

Transport Layer (TCP, UDP)

Data 3

UNDERSTANDING TCP/IP

Encapsulation of Data for Network Delivery



Application Layer

Original Message

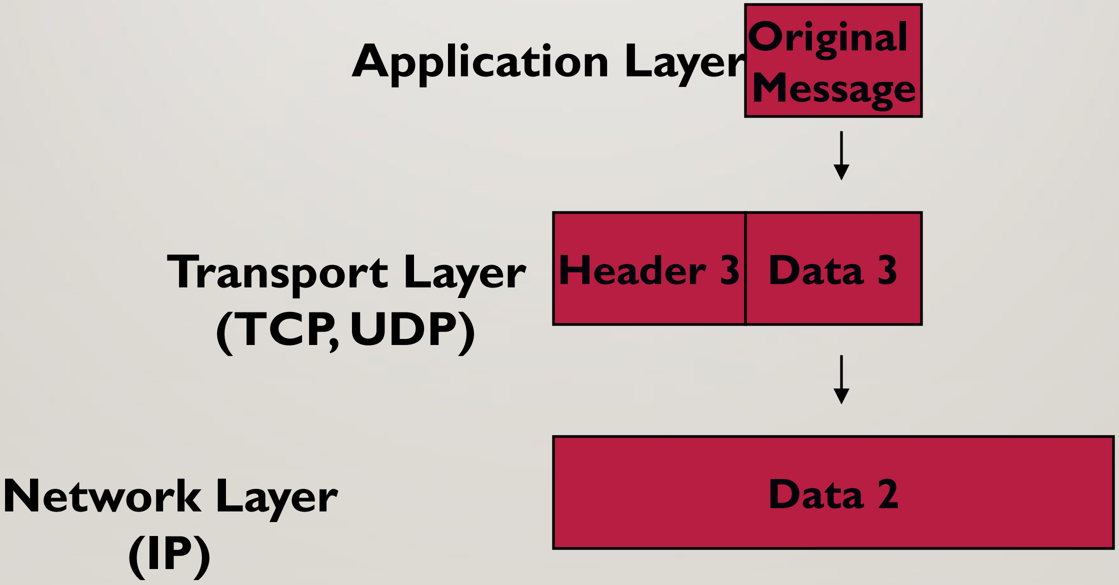
Transport Layer (TCP, UDP)

Header 3

Data 3

UNDERSTANDING TCP/IP

Encapsulation of Data for Network Delivery



Application Layer

Original Message

Transport Layer (TCP, UDP)

Header 3

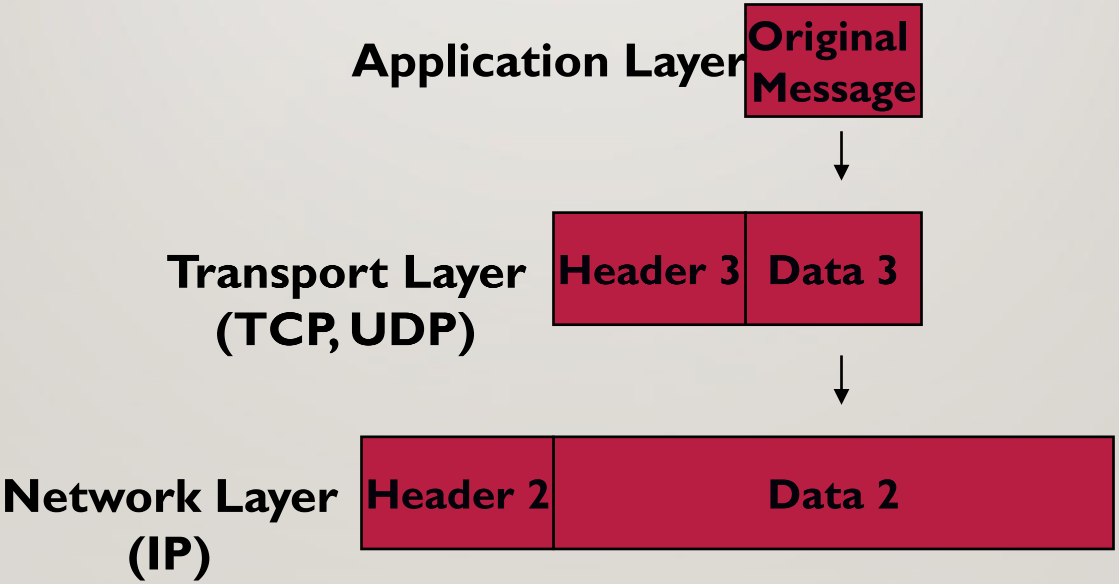
Data 3

Network Layer (IP)

Data 2

UNDERSTANDING TCP/IP

Encapsulation of Data for Network Delivery



Application Layer

Original Message

Transport Layer (TCP, UDP)

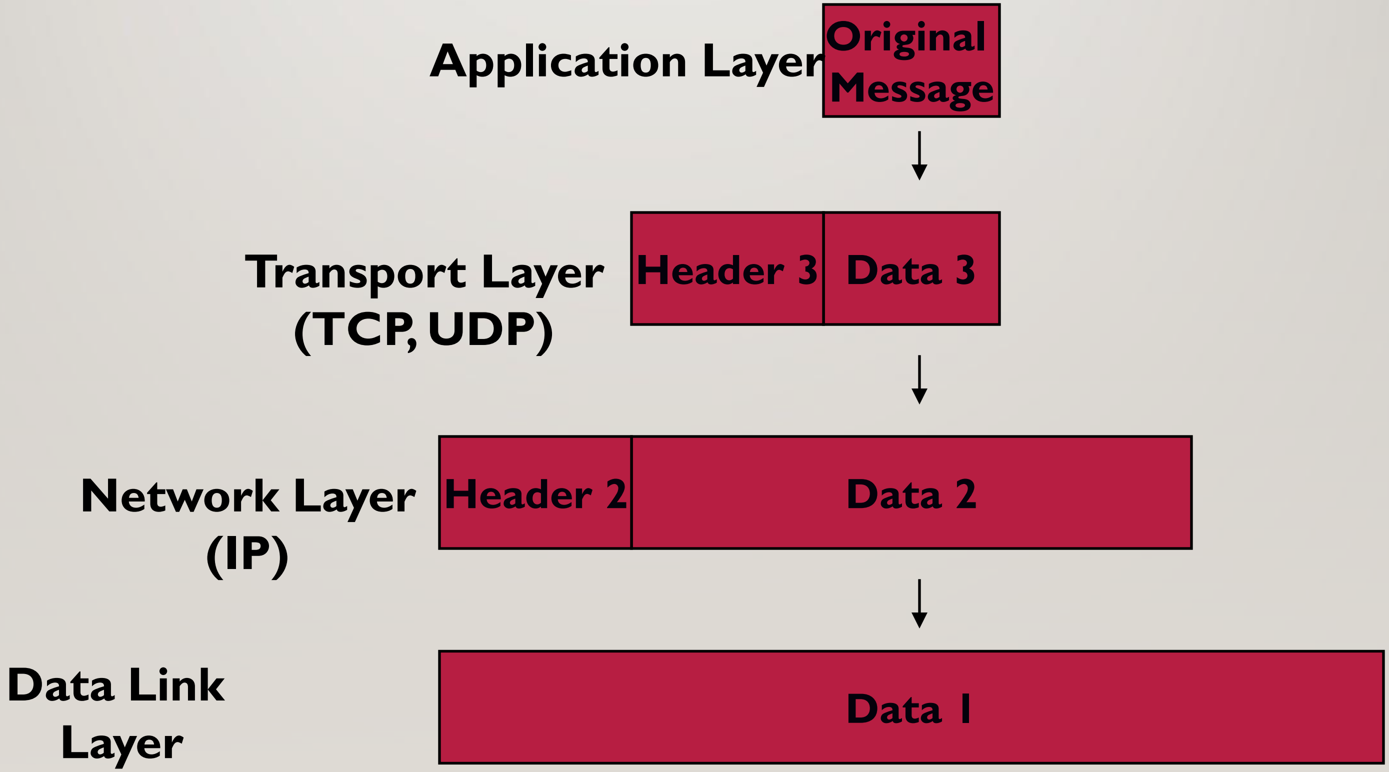
Header 3 | Data 3

Network Layer (IP)

Header 2 | Data 2

UNDERSTANDING TCP/IP

Encapsulation of Data for Network Delivery



Application Layer

Original Message

Transport Layer (TCP, UDP)

Header 3

Data 3

Network Layer (IP)

Header 2

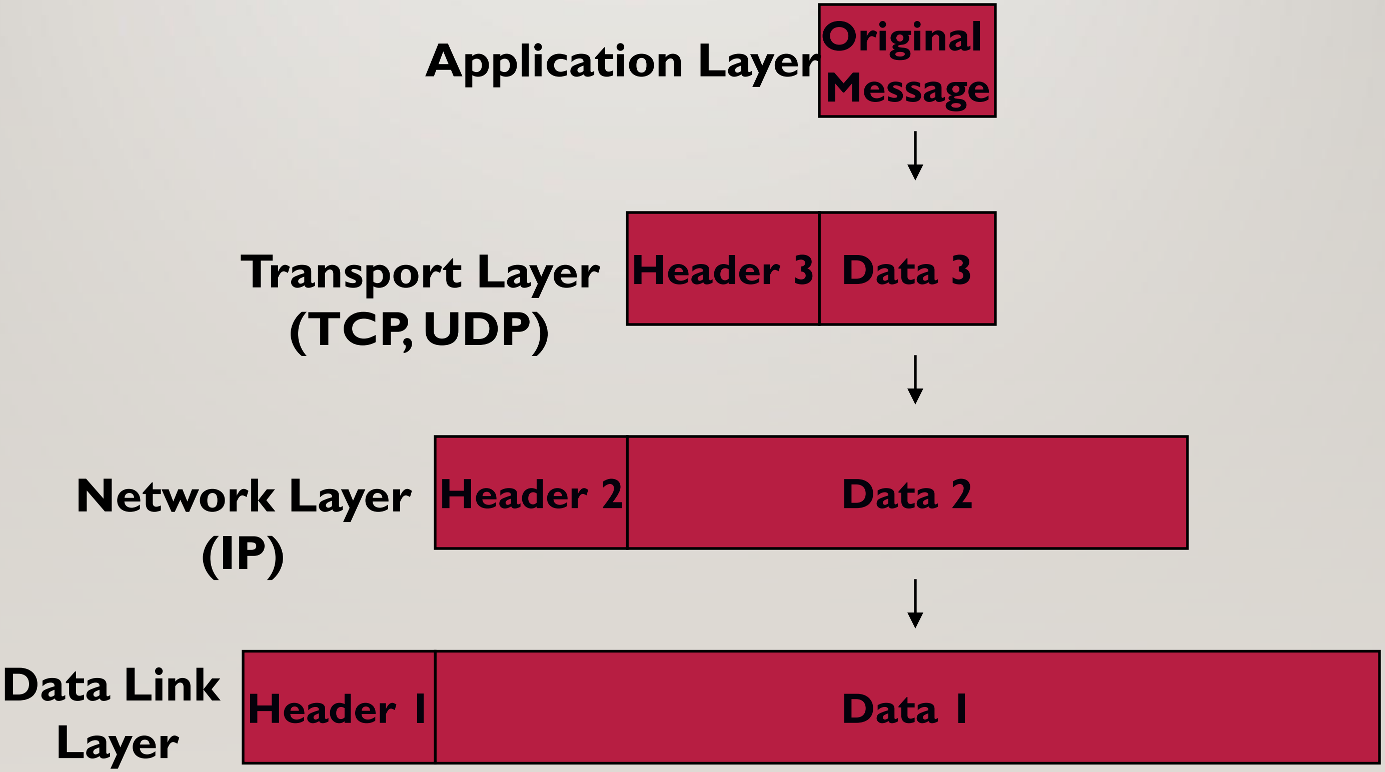
Data 2

Data Link Layer

Data 1

UNDERSTANDING TCP/IP

Encapsulation of Data for Network Delivery



Application Layer

Original Message

Transport Layer (TCP, UDP)

Header 3

Data 3

Network Layer (IP)

Header 2

Data 2

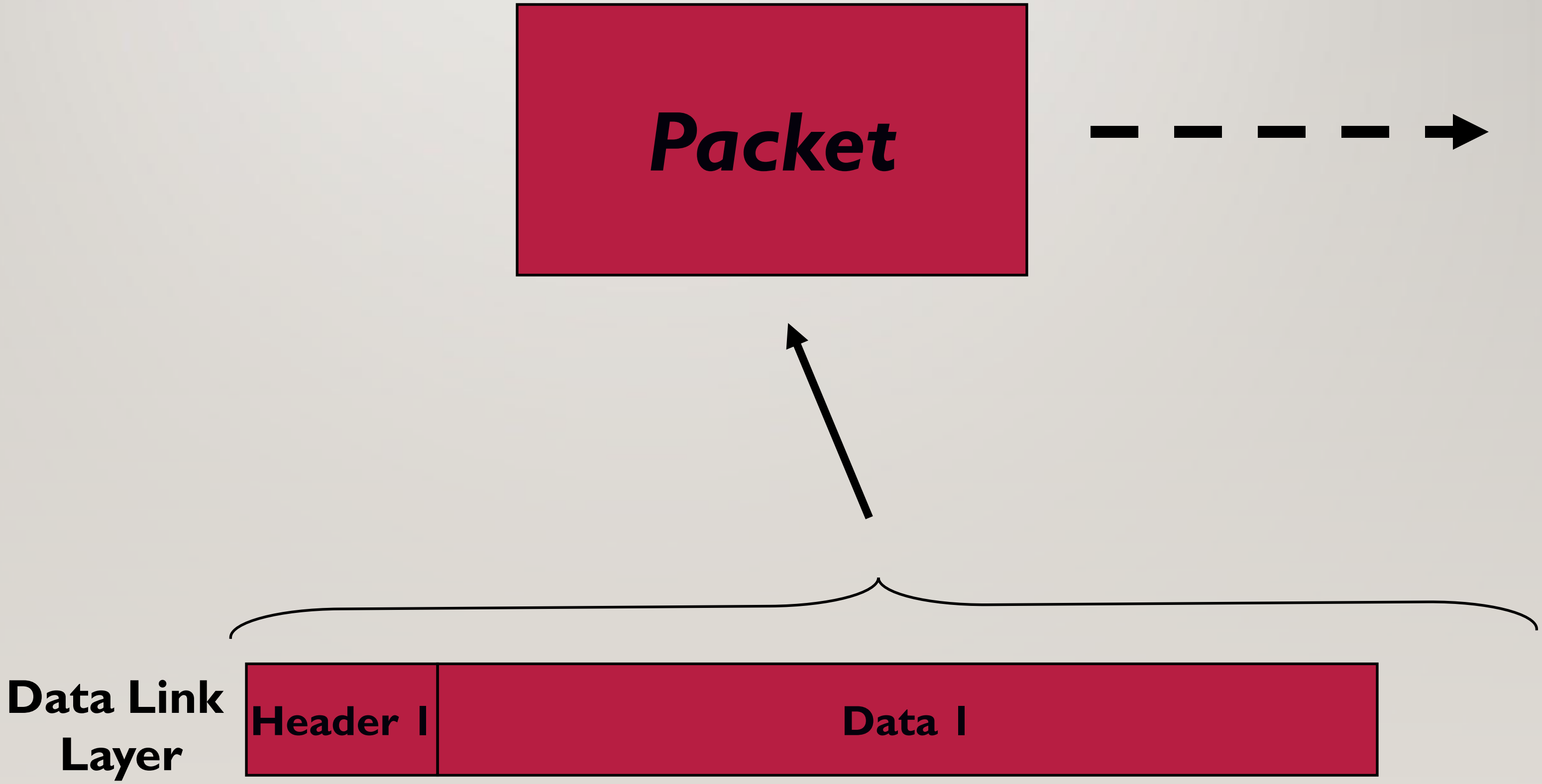
Data Link Layer

Header 1

Data 1

UNDERSTANDING TCP/IP

Packet Sent by Host A



Packet

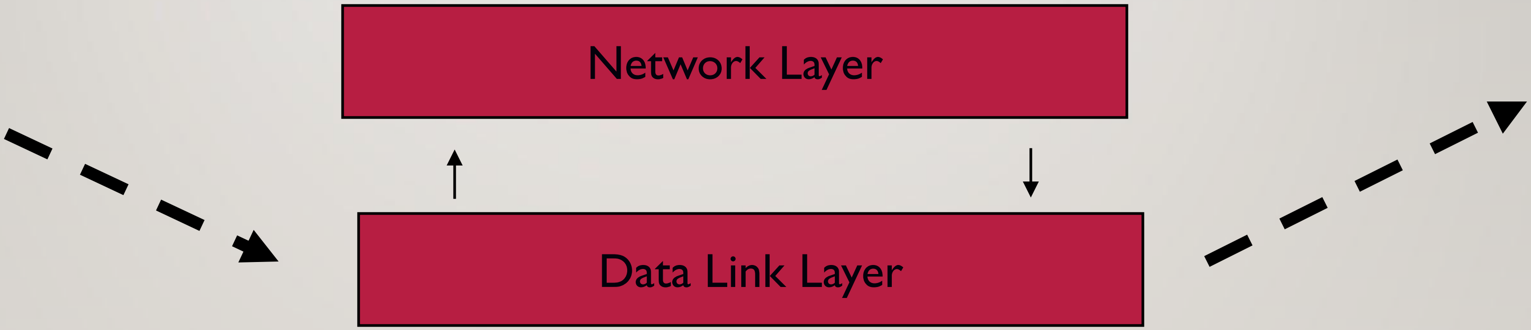
Data Link Layer

Header 1

Data 1

UNDERSTANDING TCP/IP

Packet Received by intermediary Router

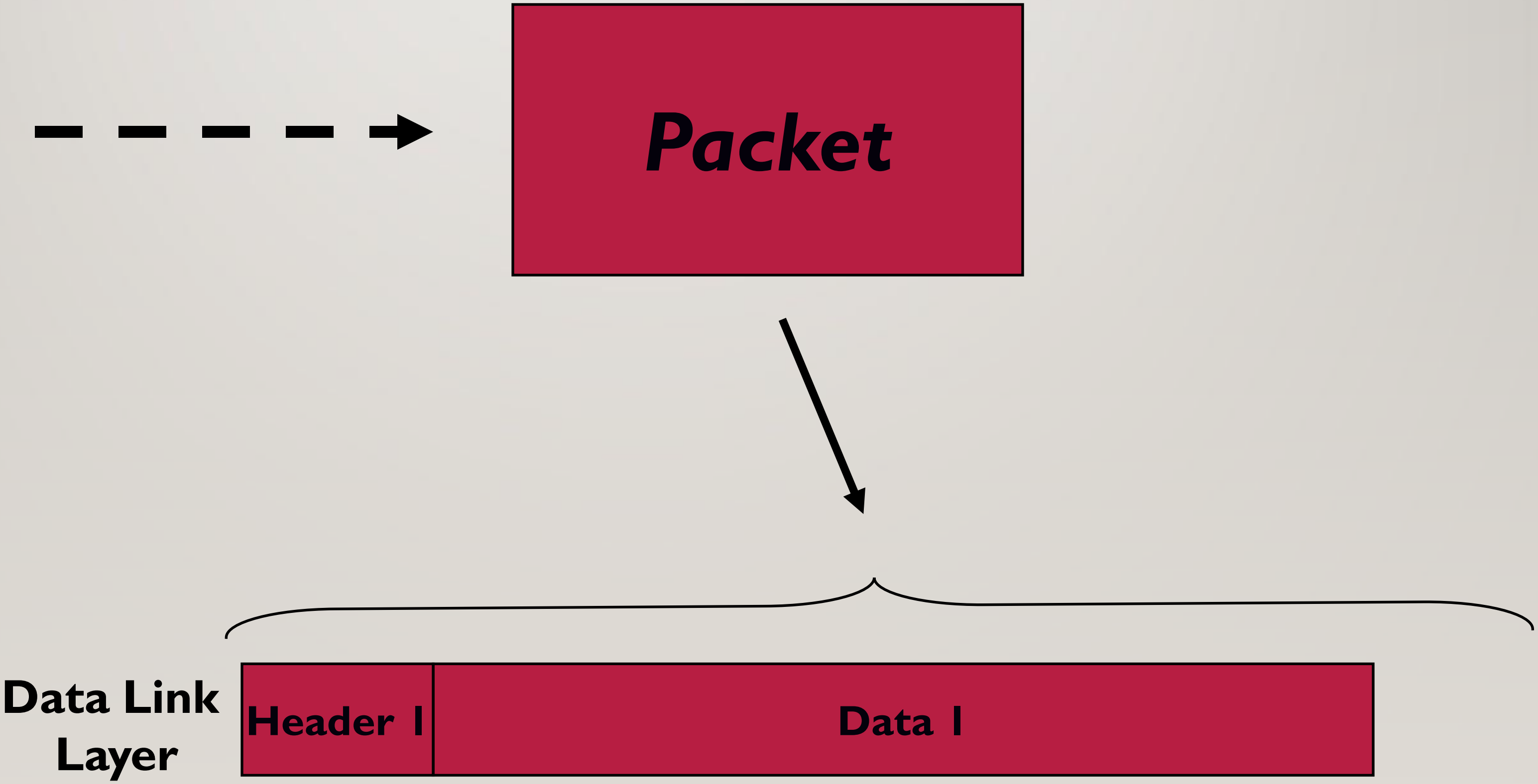


Network Layer

Data Link Layer

UNDERSTANDING TCP/IP

Packet Received by Host B



Packet

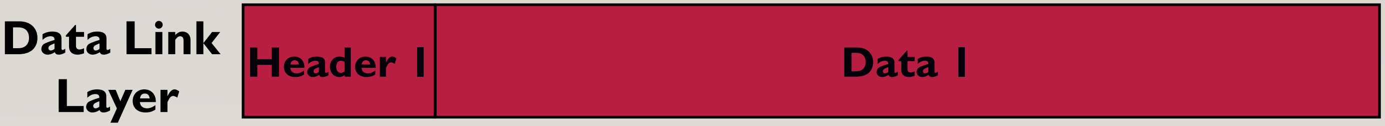
Data Link Layer

Header 1

Data 1

UNDERSTANDING TCP/IP

De-capsulation of Data from Network Delivery



Data Link Layer

Header 1

Data 1

UNDERSTANDING TCP/IP

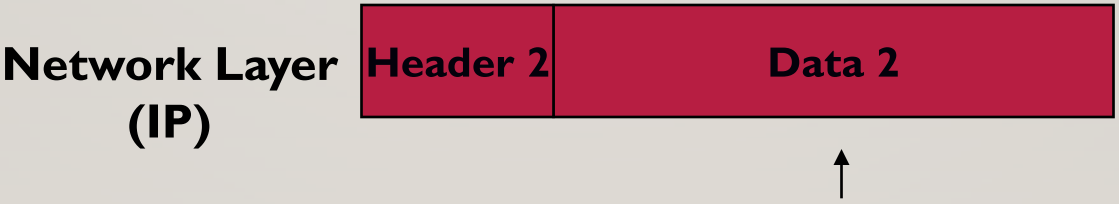
De-capsulation of Data from Network Delivery

Data Link Layer

Data 1

UNDERSTANDING TCP/IP

De-capsulation of Data from Network Delivery



UNDERSTANDING TCP/IP

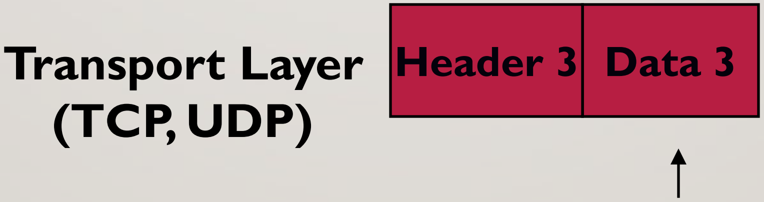
De-capsulation of Data from Network Delivery

Network Layer (IP)

Data 2

UNDERSTANDING TCP/IP

De-capsulation of Data from Network Delivery



Transport Layer (TCP, UDP)

Header 3

Data 3

UNDERSTANDING TCP/IP

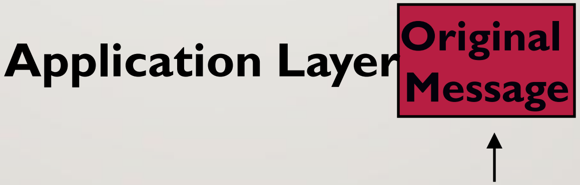
De-capsulation of Data from Network Delivery

Transport Layer (TCP, UDP)

Data 3

UNDERSTANDING TCP/IP

De-capsulation of Data from Network Delivery



Application Layer

Original Message

UNDERSTANDING TCP/IP

De-capsulation of Data from Network Delivery

Application Layer **Original Message**

SECURITY AT WHAT LEVEL?

Application Layer	PGP, Kerberos, SSH, etc.
Transport Layer	Transport Layer Security (TLS)
Network Layer	IP Security
Data Link Layer	Hardware encryption

SECURITY AT APPLICATION LAYER

(PGP, Kerberos, SSH, etc.)

- Implemented in end-hosts
- Advantages
  - Extend application without involving operating system.
  - Application can understand the data and can provide the appropriate security.
- Disadvantages
  - Security mechanisms have to be designed independently of each application.

SECURITY AT TRANSPORT LAYER

Transport Layer Security (TLS)

- Implemented in end-hosts
- Advantages
- Existing applications get security seamlessly
- Disadvantages
- Protocol specific

SECURITY AT NETWORK LAYER

IP Security (IPSec)

- Advantages
- Provides seamless security to application and transport layers (ULPs).
- Allows per flow or per connection security and thus allows for very fine-grained security control.
- Disadvantages
- More difficult to to exercise on a per user basis on a multi-user machine.

SECURITY AT DATA LINK LAYER

- (Hardware encryption)
- Need a dedicated link between host/routers.

- Advantages

- Speed.

- Disadvantages

- Not scalable.
- Need dedicated links.

IP SECURITY (IPSEC)

- IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF).

Creates **secure, authenticated, reliable communications over IP networks**

IPSEC SECURITY SERVICES

- Connectionless integrity

  Assurance that received traffic has not been modified. Integrity includes anti-reply defenses.

- Data origin authentication

  Assurance that traffic is sent by legitimate party or parties.

- Confidentiality (encryption)

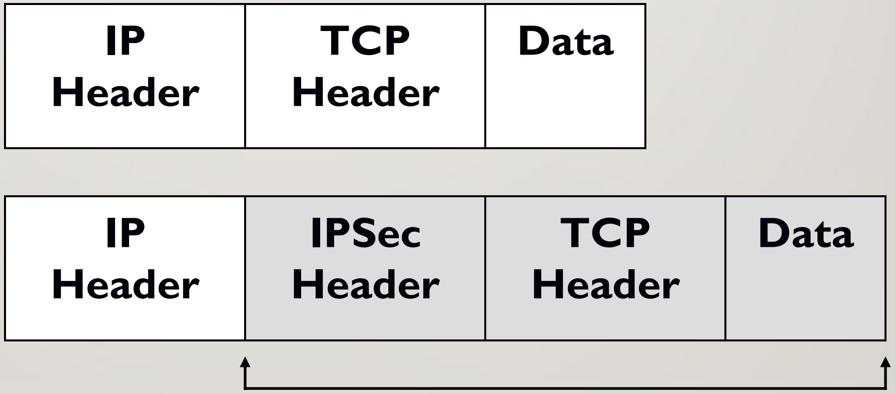
  Assurance that user's traffic is not examined by non-authorized parties.

- Access control

  Prevention of unauthorized use of a resource.

IPSEC MODES OF OPERATION

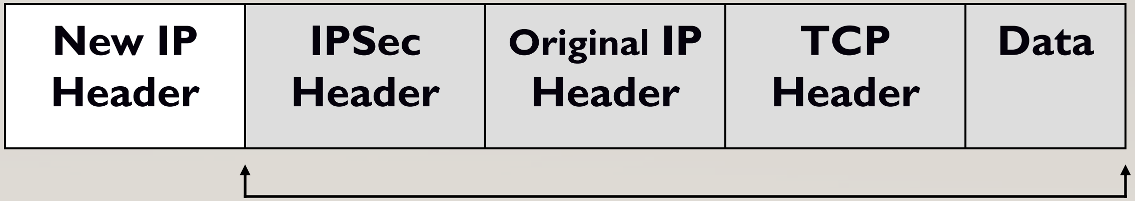
- Transport Mode: protect the upper layer protocols



Original IP Datagram	**IP Header**	**TCP Header**	**Data**	
Transport Mode protected packet	**IP Header**	**IPSec Header**	**TCP Header**	**Data**

protected

- Tunnel Mode: protect the entire IP payload

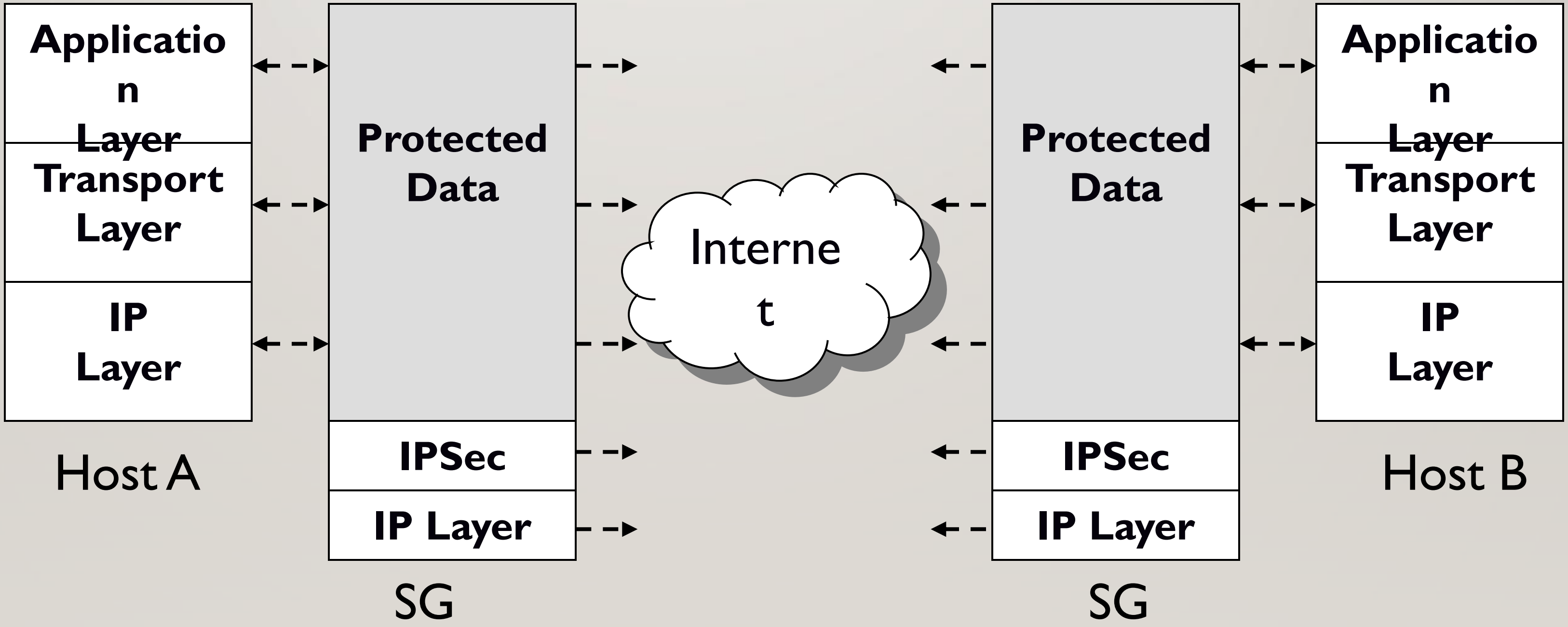


Tunnel Mode protected packet	**New IP Header**	**IPSec Header**	**Original IP Header**	**TCP Header**	**Data**

protected

TUNNEL MODE

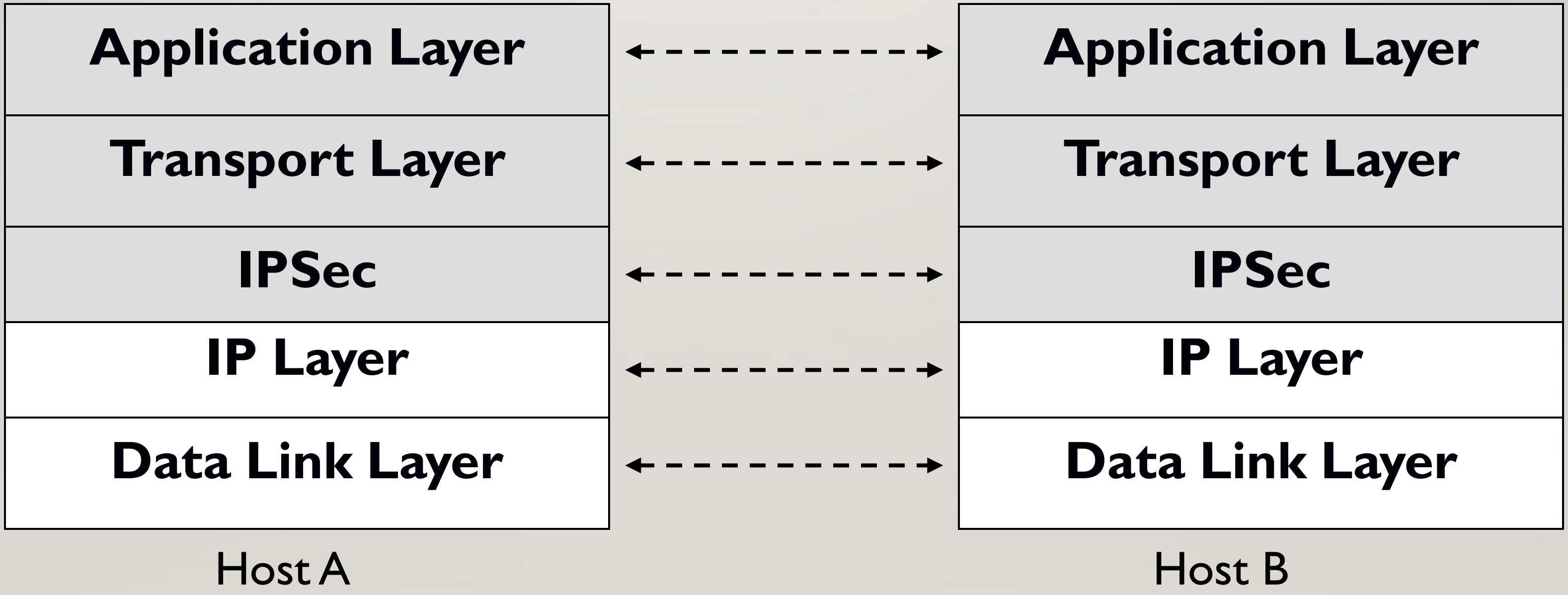
- Host-to-Network, Network-to-Network



SG = Security Gateway

TRANSPORT MODE

- Host-to-Host



Application Layer	Application Layer
Transport Layer	Transport Layer
IPSec	IPSec
IP Layer	IP Layer
Data Link Layer	Data Link Layer
Host A	Host B

IPSEC SECURITY PROTOCOLS

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

IPSEC SECURITY PROTOCOLS

- Authentication Header (AH) provides:

- Connectionless integrity

- Data origin authentication

- Protection against replay attacks

- Encapsulating Security Payload (ESP) provides:

- Confidentiality (encryption)

- Connectionless integrity

- Data origin authentication

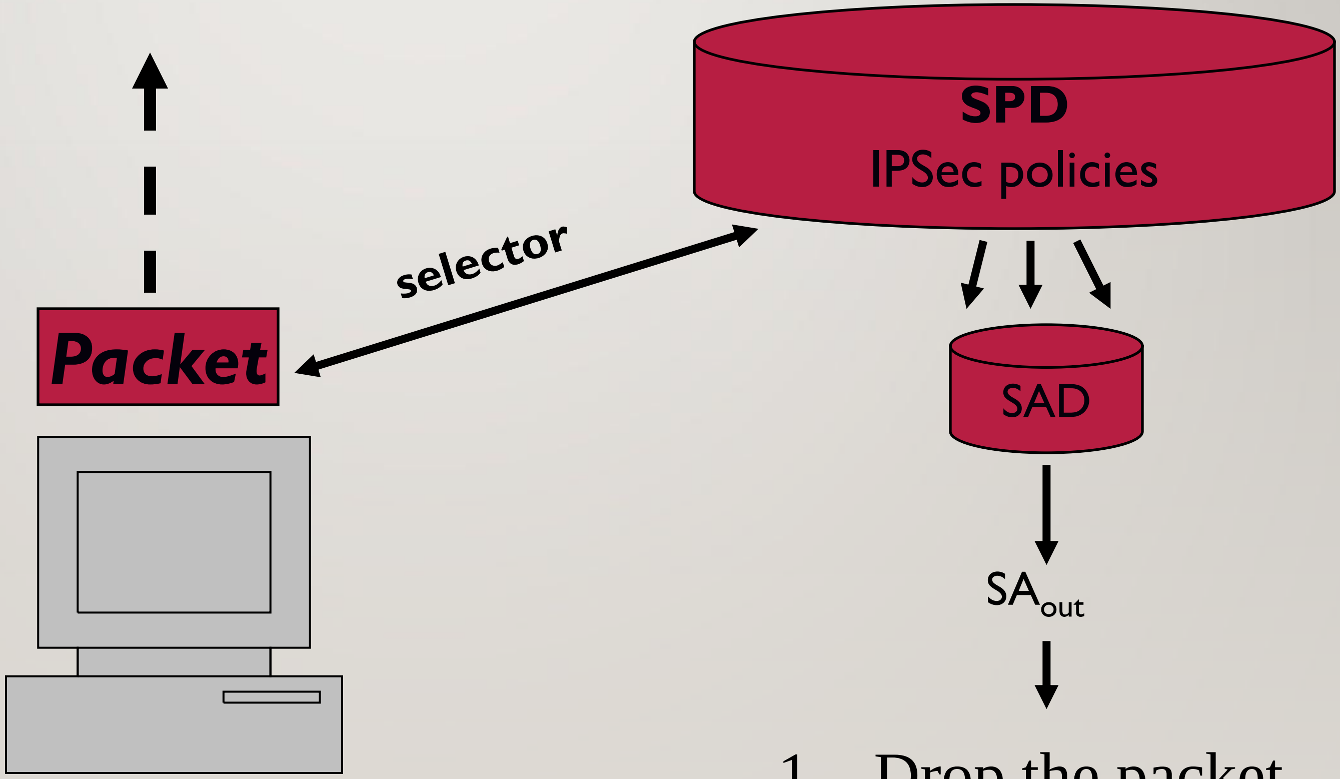
- Protection against reply attacks

- Both protocols may be used alone or applied in combination with each other.

OUTBOUND/INBOUND IPSEC PROCESSING

- The inbound and the outbound IPSec processing are completely independent.

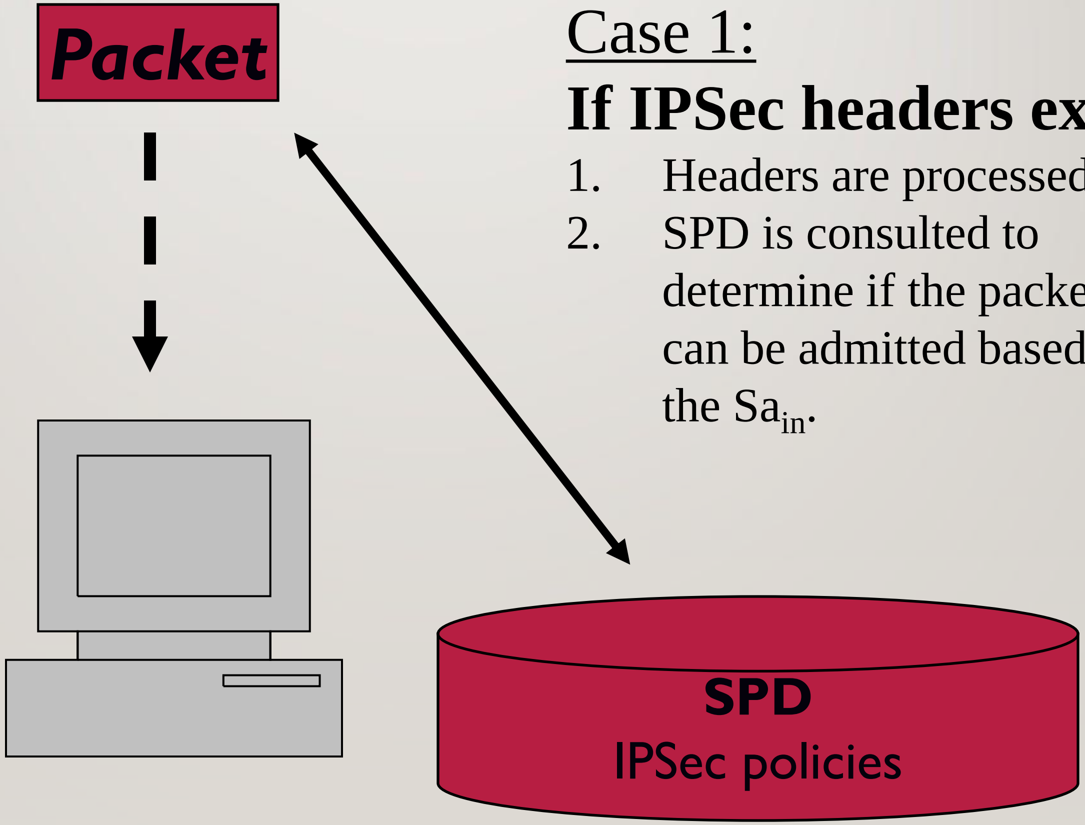
OUTBOUND IPSEC PROCESSING



1. Drop the packet.
2. Bypass IPSec.
3. Apply IPSec.

SPD = Security Policy Database
SAD = Security Association Database
SA = Security Association

INBOUND IPSEC PROCESSING



Packet

SPD

IPSec policies

Case 1:

If IPSec headers exists

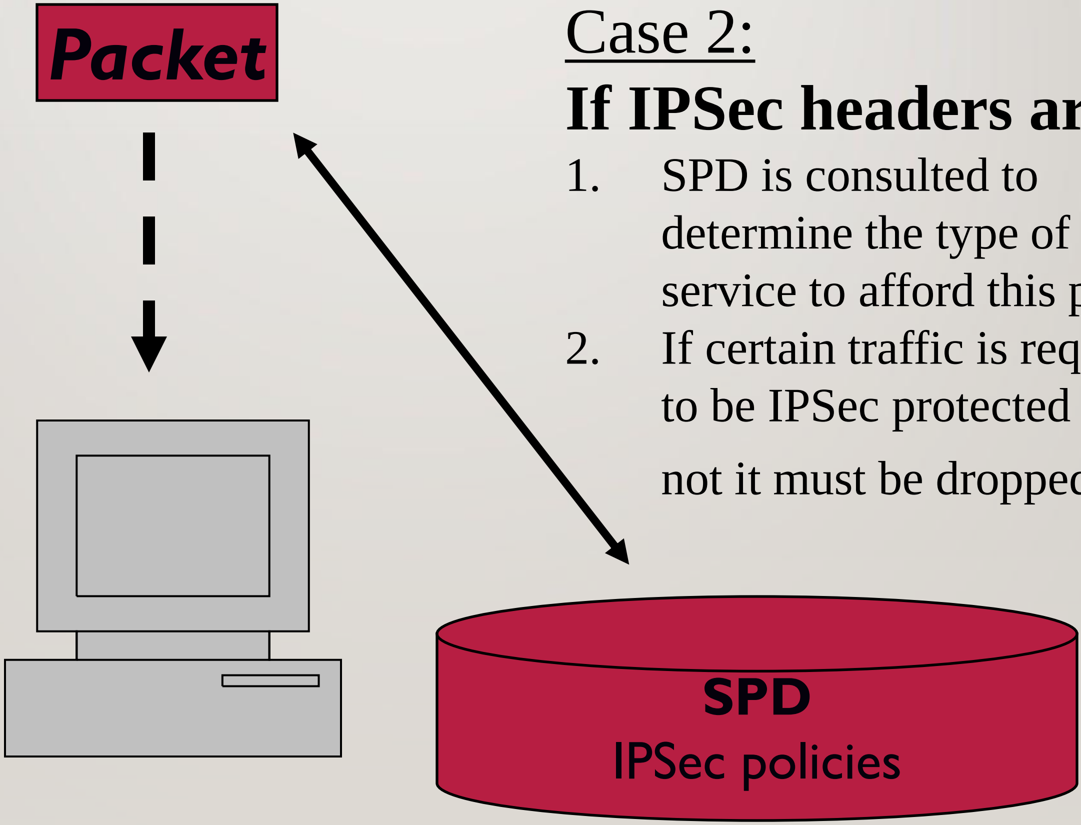
1. Headers are processed.
2. SPD is consulted to determine if the packet can be admitted based on the Sa_{in}.

SPD = Security Policy Database

SAD = Security Association Database

SA = Security Association

INBOUND IPSEC PROCESSING



Case 2:

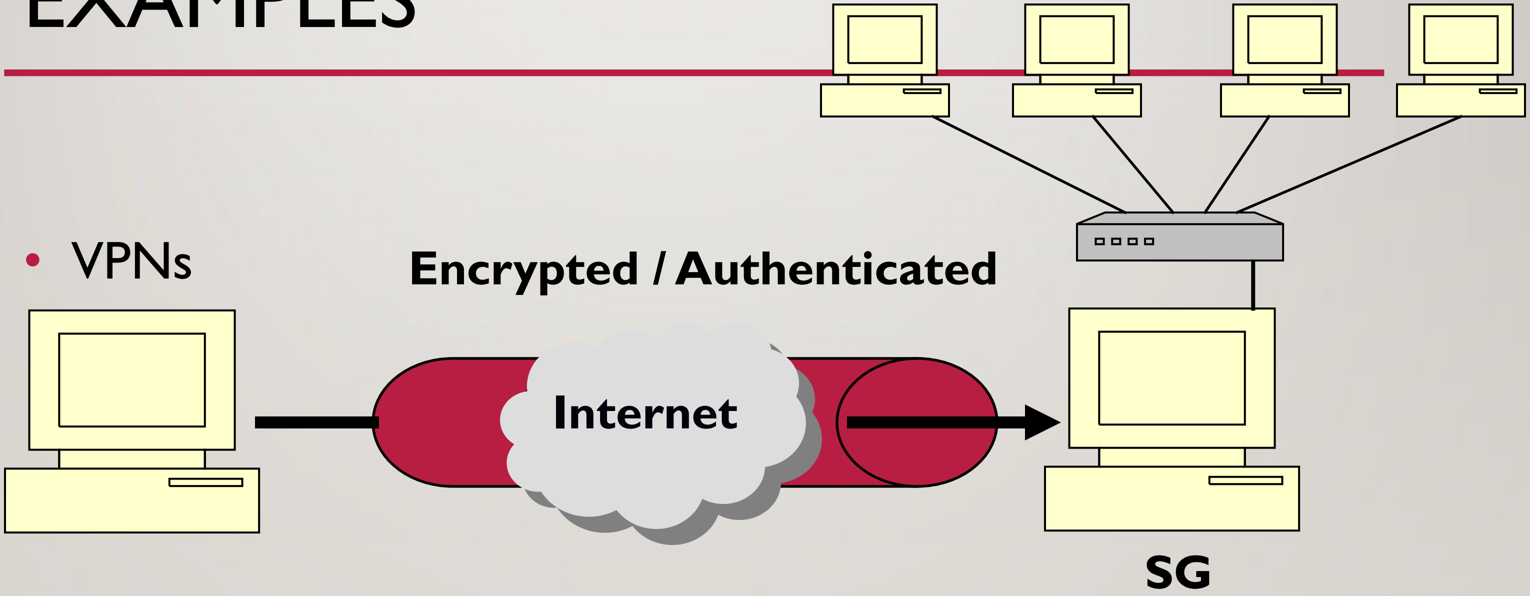
If IPSec headers are absent

1. SPD is consulted to determine the type of service to afford this packet.
2. If certain traffic is required to be IPSec protected and its not it must be dropped.

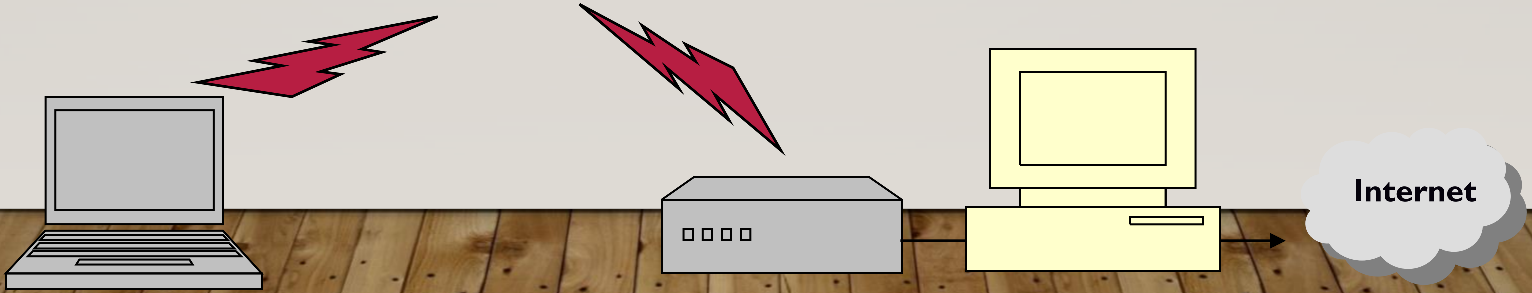
SPD = Security Policy Database
SAD = Security Association Database
SA = Security Association

REAL WORLD DEPLOYMENT EXAMPLES

- VPNs



- Wireless



CONCLUSION

- **The Internet was not created with security in mind.**
- Communications can be altered, examined and exploited.
- There is a growing need to protect **private information** crossing the **public networks** that make up the Internet infrastructure.
- IPSec is a set of protocols and methodologies to create secure IP connections.

QUESTIONS?