Chap. 13 Cryptography and Network Security

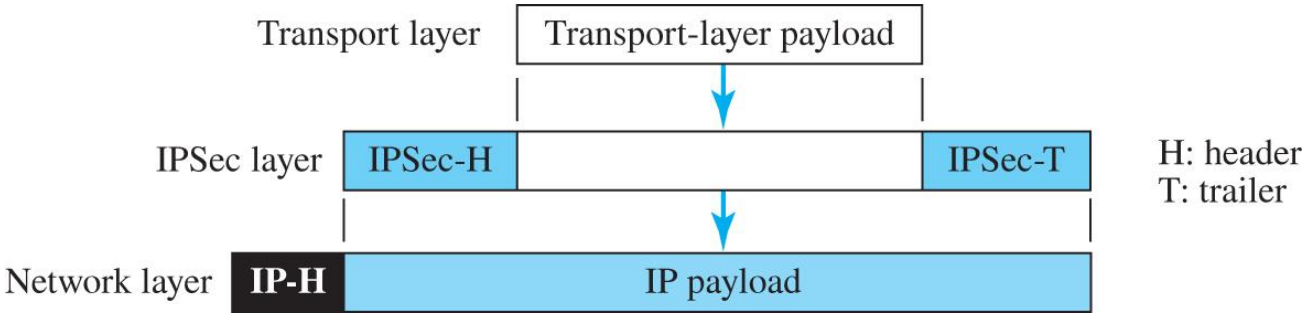
SungKongHoe University
Major of Computer Science and Engineering
Yeonsik Jeong

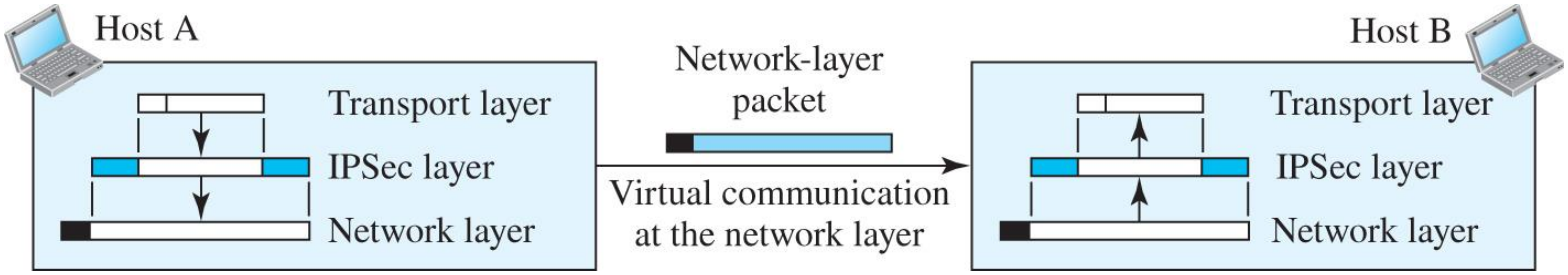
Contents

- Introduction
- Confidentiality
- Other Aspects of Security
- ✓ Network-Layer Security
- Transport-Layer Security
- Application-Layer Security
- Firewalls

Network-Layer Security

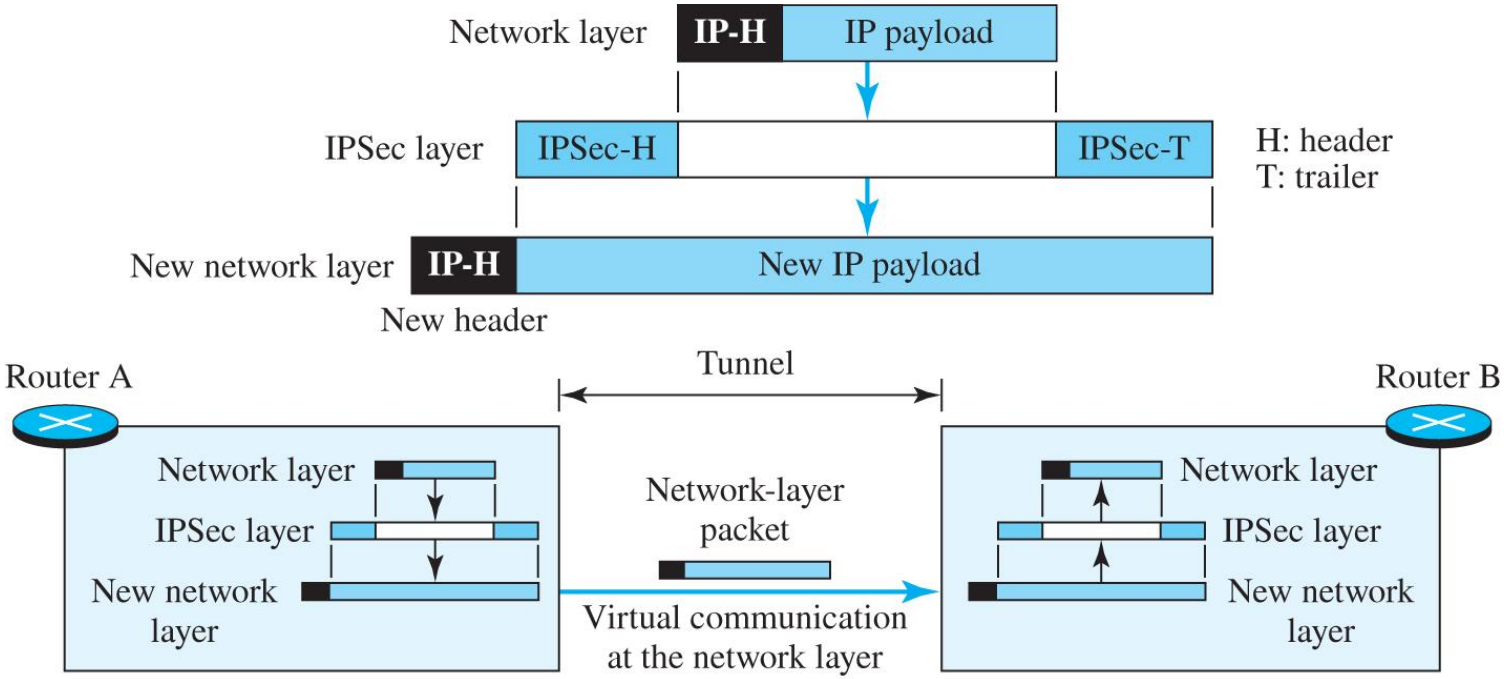
- **IPSec (IP Security)**
  - **Transport mode**
    - Protects the payload to be encapsulated in the network layer, but does not protect the IP header
    - Normally used when we need host-to-host (end-to-end) protection of data





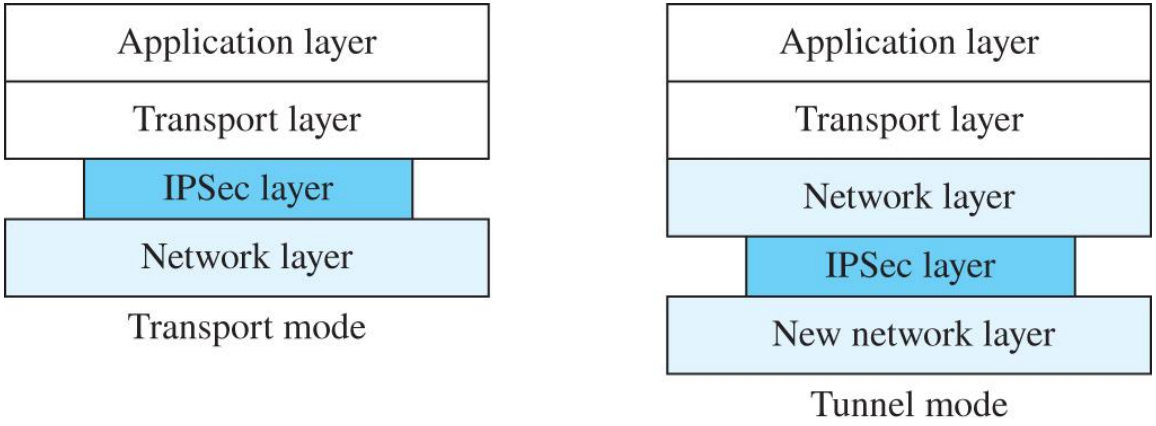
Network-Layer Security

- **IPSec (IP Security)**
  - **Tunnel mode**
    - Takes an IP packet, including the header, applies IPSec security methods to the *entire* packet and adds a new IP header
    - Normally used between two routers, between a host and a router



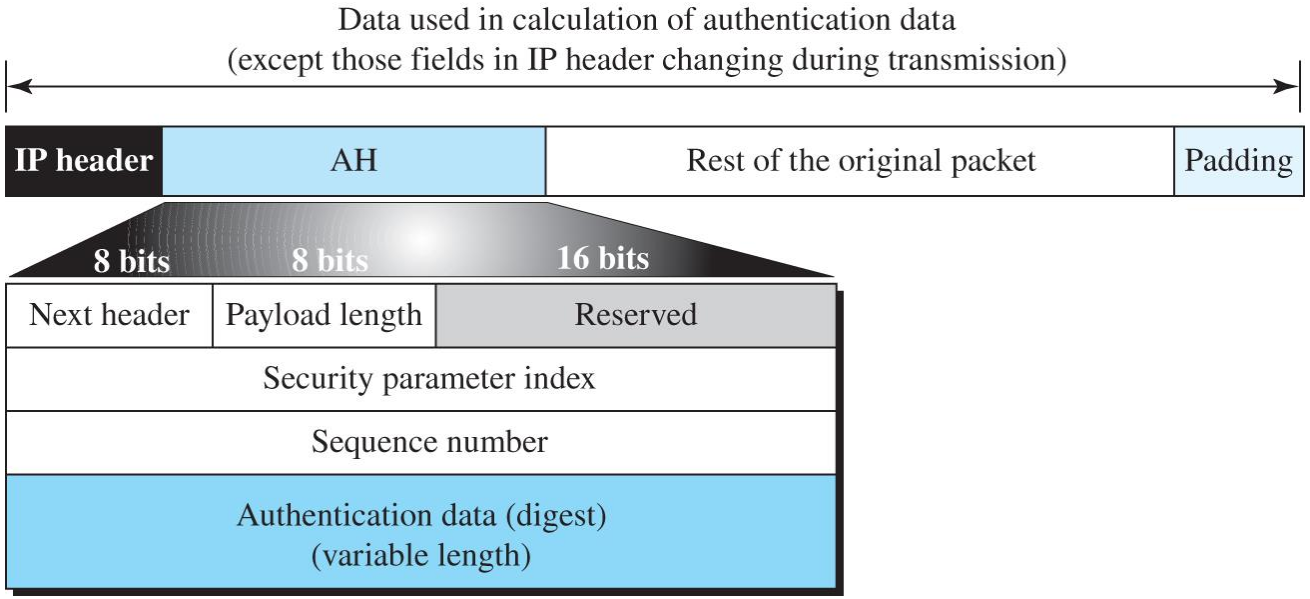
Network-Layer Security

- **IPSec (IP Security)**
  - **Transport mode vs. Tunnel mode**
    - In transport mode, the IPSec layer comes between the transport layer and the network layer
    - In tunnel mode, the flow is from the network layer to the IPSec layer and then back to the network layer again



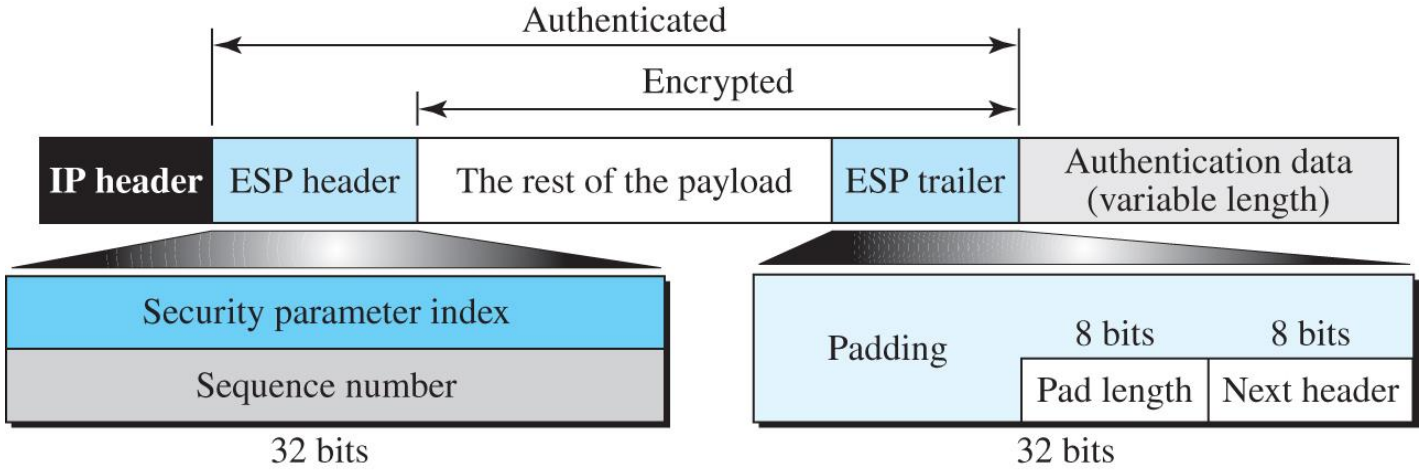
Network-Layer Security

- **IPSec (IP Security)**
  - **Authentication Header (AH)**
    - Designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet
    - Uses a hash function and a symmetric (secret) key to create a message digest; the digest is inserted in the authentication header (see MAC).



Network-Layer Security

- **IPSec (IP Security)**
  - **Encapsulating Security Payload (ESP)**
    - Provides source authentication, integrity, and *confidentiality*
    - Adds a header and trailer
    - ESP's authentication data are added at the end of the packet
    - ESP does whatever AH does with additional functionality (confidentiality)



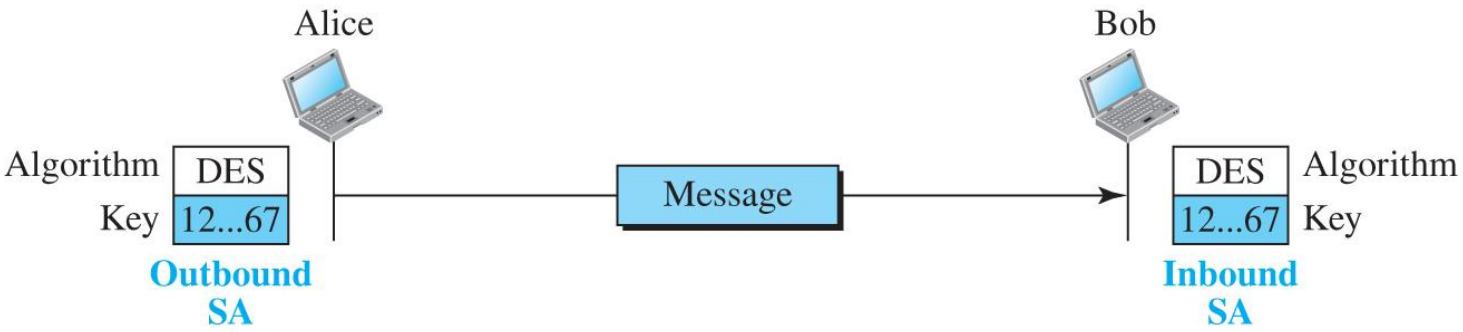
Network-Layer Security

- **IPSec (IP Security)**
  - **AH vs. ESP**
    - The ESP was designed after the AH was already in use
    - The ESP does whatever AH does with additional functionality (confidentiality), so the AH actually is not needed
  - **Services provided by AH and ESP**

Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

Network-Layer Security

- **IPSec (IP Security)**
  - **Security Association (SA)**
    - A SA is a contract between two parties; it creates a secure channel between them
    - The SA changes the connectionless service provided by IP to a connection-oriented service upon which we can apply security
    - The SA can be much more complex if the parties need to use specific algorithms and specific parameters for different protocols, such as IPSec AH or IPSec ESP



Network-Layer Security

- **IPSec (IP Security)**
  - **Security Association Database (SAD)**
    - Each site needs to have both inbound and outbound SAs to allow bidirectional communication
    - Normally, there are two SADs, one inbound and one outbound
    - Each entry in a SAD is selected using a triple index: *security parameter index* (a 32-bit number that defines the SA at the database), *destination address*, and *protocol* (AH or ESP)

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
• • •	
< SA, DA, Name, P, SPort, DPort >	

SA: Source address
DA: Destination address
P: Protocol
SPort: Source port
DPort: Destination port

Network-Layer Security

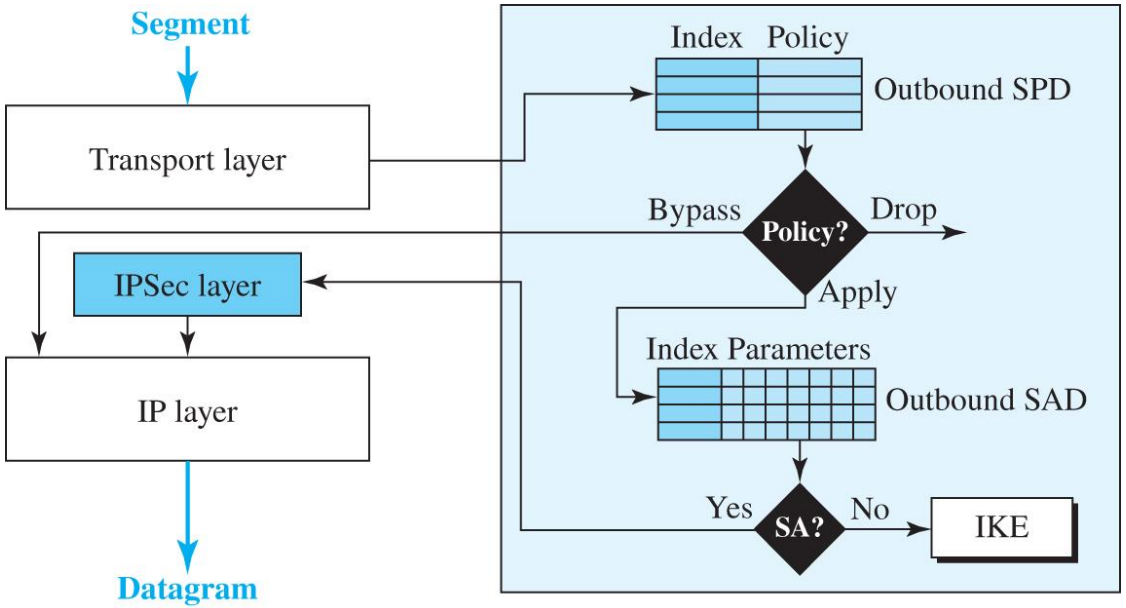
- **IPSec (IP Security)**
  - **Security Policy (SP)**
    - Defines the type of security applied to a packet when it is to be sent or when it has arrived
    - Before using the SAD, a host must determine the predefined policy for the packet
  - **Security Policy Database (SPD)**
    - There is a need for an inbound SPD and an outbound SPD
    - Each entry in the SPD can be accessed using a sextuple index

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
• • •	
< SA, DA, Name, P, SPort, DPort >	

SA: Source address
DA: Destination address
P: Protocol
SPort: Source port
DPort: Destination port

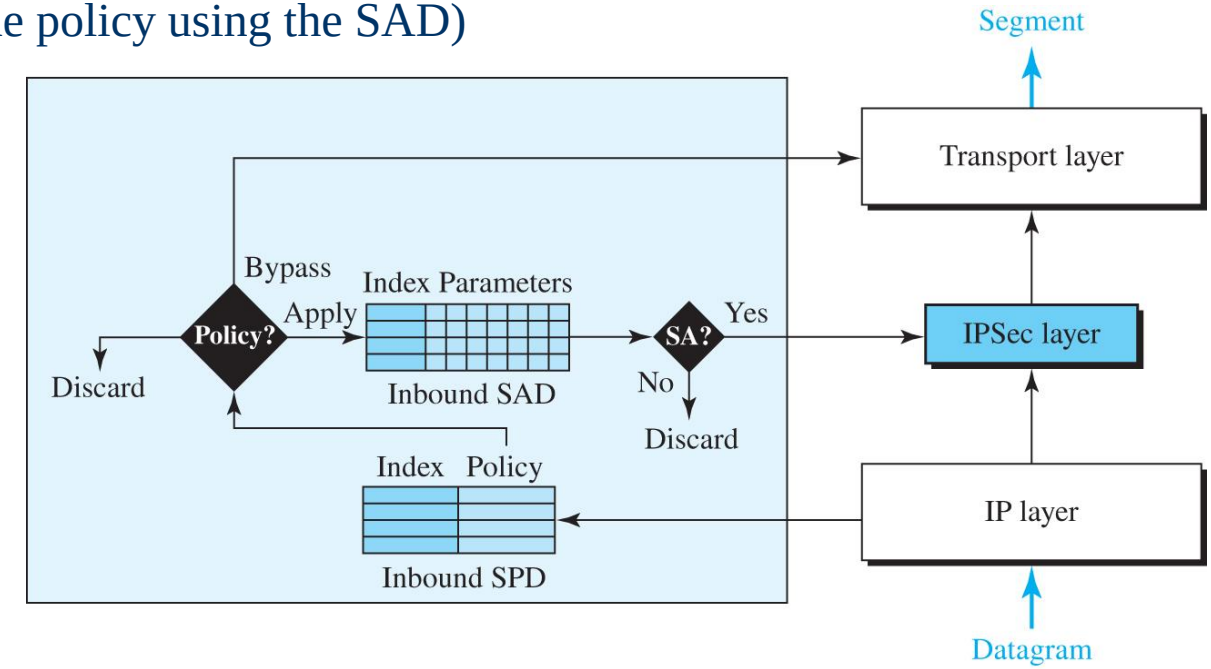
Network-Layer Security

- **IPSec (IP Security)**
  - **Outbound SPD**
    - The input to the outbound SPD is the sextuple index
    - The output is one of the cases: *drop* (packet cannot be sent), *bypass* (bypassing security header), and *apply* (applying the security according to the SAD, if no SAD, creating one)



Network-Layer Security

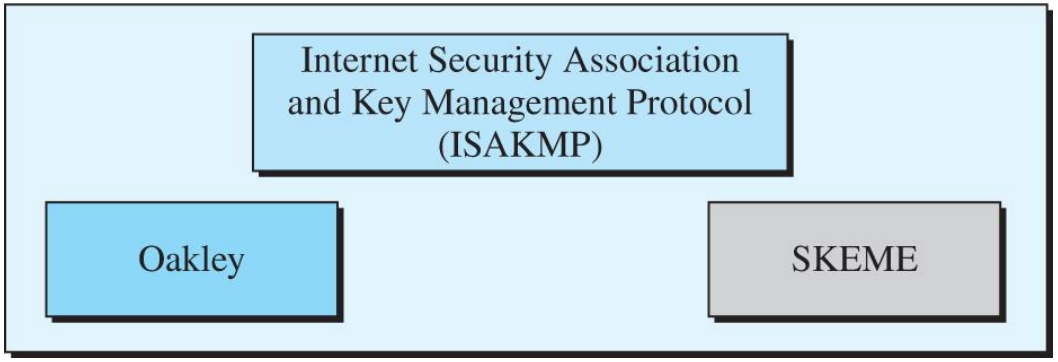
- **IPSec (IP Security)**
  - **Inbound SPD**
    - The input to the inbound SPD is the sextuple index
    - The output is one of the cases: *discard* (drop the packet), *bypass* (bypassing the security and delivering the packet to the transport layer), and *apply* (applying the policy using the SAD)



Network-Layer Security

- **IPSec (IP Security)**
  - **Internet Key Exchange (IKE)**
    - A protocol designed to create both inbound and outbound Sas
    - If there is no SA, IKE is called to establish a SA
    - A complex protocol based on three other protocols: Oakley, SKEME, ISAKMP

Internet Key Exchange (IKE)



Network-Layer Security

- **IPSec (IP Security)**
  - **Virtual Private Network (VPN)**
    - The network is physically public but virtually private
    - VPN technology uses the *ESP* protocol of IPSec in the *tunnel* mode