IP Security (IPSec)

Network Security (NETSEC)

Yuhong Li

Stockholm University

Outline

- Overview
- IPSec security constructs
  - IPSec Policy
  - Security Associations (SA)
  - Security Parameter Index (SPI)
  - IPSec modes (Transport + Tunnel)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)
- IPSec Internet Key Exchange (IKE)

Cryptographic Primitives vs. Cryptographic Systems

- Cryptographic primitives
  - The most basic building blocks for cryptographic systems
  - Example: SHA3-512, RSA, AES, DSS
- Cryptographic systems
  - Systems made up of several cryptographic primitives
  - Examples: IPSec, SSL/TLS, SSH

Overview

Fundamental Issues

- Things to think about for securing the network
  - What are the vulnerabilities?
  - How they affect the overall risk state of the network, and how to assess that state.
- Both are necessary to develop security policy that actually defines the measures to be considered and eventually implemented

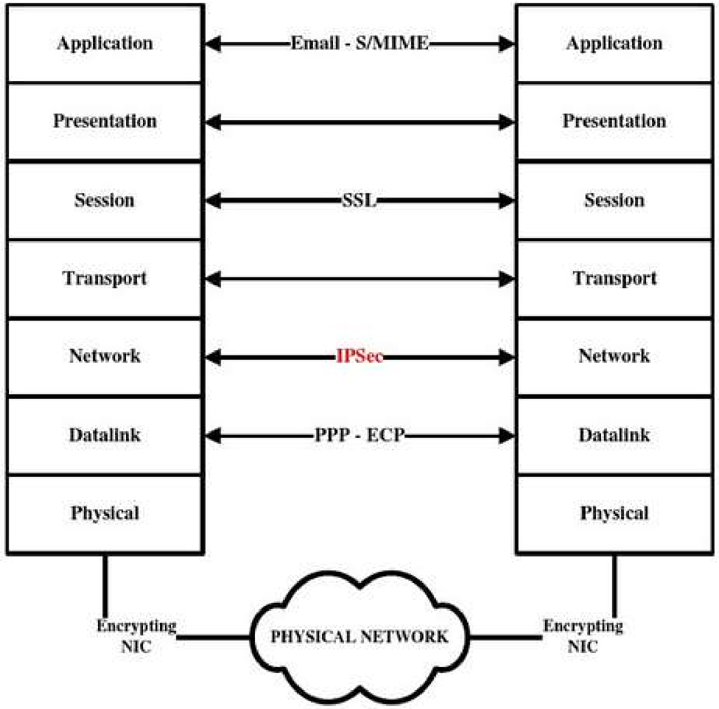
The IAB Initiative(1994)

- Internet Architecture Board (IAB) in the report published 1994 (RFC 1636) stated that
  - The Internet needs much more and better security
  - Mechanisms should exist to
    - Prevent the network infrastructure from unauthorized monitoring and control
    - Make it possible to secure the E2E traffic via authentication and encryption mechanisms
  - The mechanisms should be incorporated into the next generation IP protocols, such as IPv6. Nevertheless, provisions should be made that IPv4 also benefits from the development (and it does).

The IAB Initiative and IPSec

- The IAB also stated that:
  - All IP datagrams sent over the Internet should be authenticated, in order to prevent IP spoofing and connection hijacking, as well as to secure the content of IP datagrams against any unauthorized modifications.
  - In order to guarantee privacy, all IP datagrams sent over the Internet should be encrypted by employing strong cryptography.
  - It is desirable to have both encryption and authentication applied to IP datagrams.

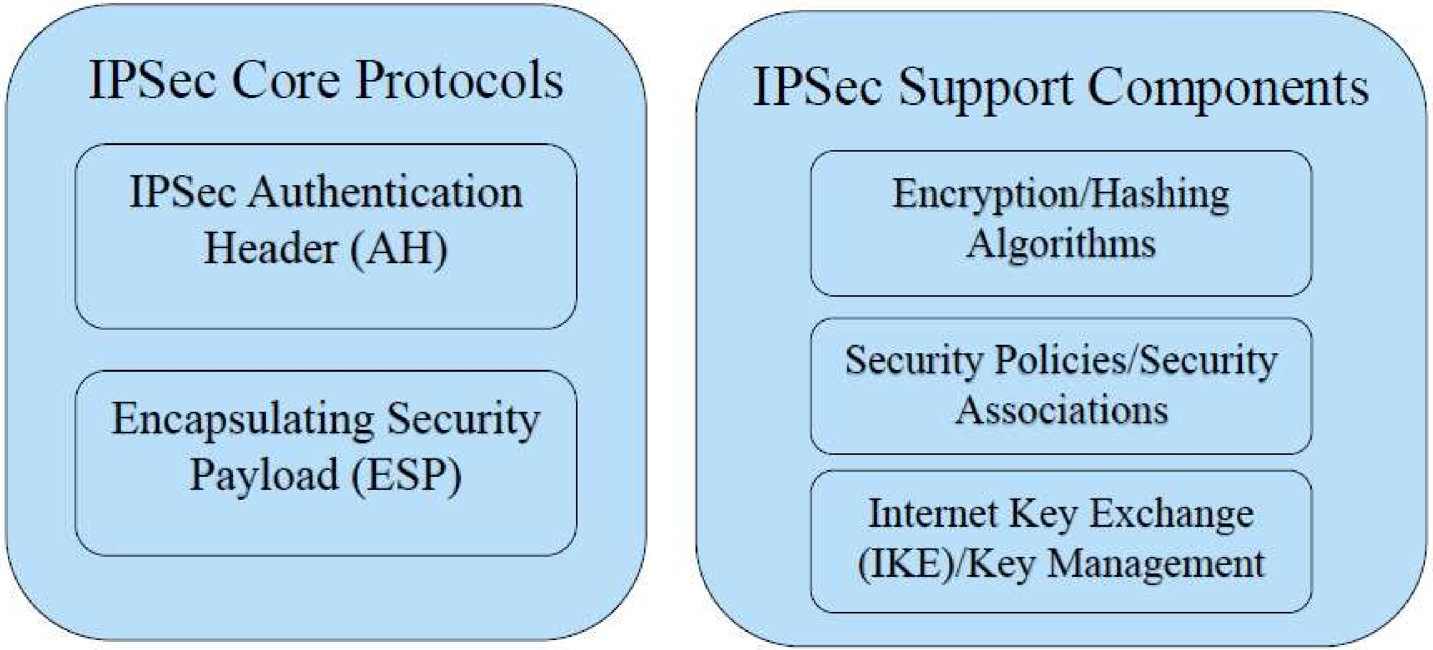
Security Protocol Layers



IPSec allows you to

- Secure communications across a LAN, WANs, and the Internet
  - Secure branch office connectivity
  - Secure remote access over the Internet
- Secure communication with other organizations: authentication and confidentiality and a key exchange mechanism
- Enhance e-commerce security: IPsec guarantees that all traffic designated by the network administrator is both encrypted and authenticated
  - Encrypt and/or authenticate all traffic at the IP level

The IPSec Protocol Suite



IPSec Core Protocols

IPSec Authentication Header (AH)

Encapsulating Security Payload (ESP)

IPSec Support Components

Encryption/Hashing Algorithms

Security Policies/Security Associations

Internet Key Exchange (IKE)/Key Management

IPSec Functional Areas

- IPsec encompasses three functional areas:
  - Authentication: makes use of the HMAC message authentication code.
    - can be applied to the entire original IP packet (tunnel mode) or to all of the packet except for the IP header (transport mode).
  - Confidentiality: provided by an encryption format known as encapsulating security payload.
    - Both tunnel and transport modes can be accommodated.
  - Key management: IKE (Internet Key Exchange)

IPSec Standards

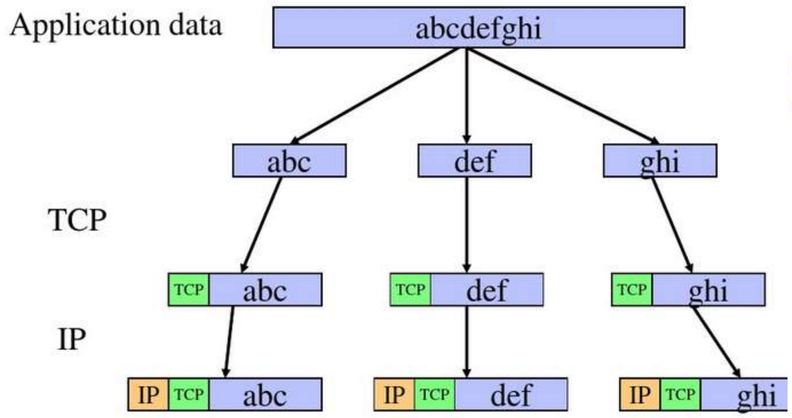
- RFC 4301 -The IP Security Architecture
- RFC 4302 -defines Authentication Header(AH)
- RFC 4303 -defines Encapsulating Security Payload(ESP)
- RFC 2408 ISAKMP -Internet Security Association and Key Management Protocol
- RFC 5996 IKE v2
- RFC 4835 Cryptographic Algorithm Implementation for ESP and AH

IPSec Capabilities

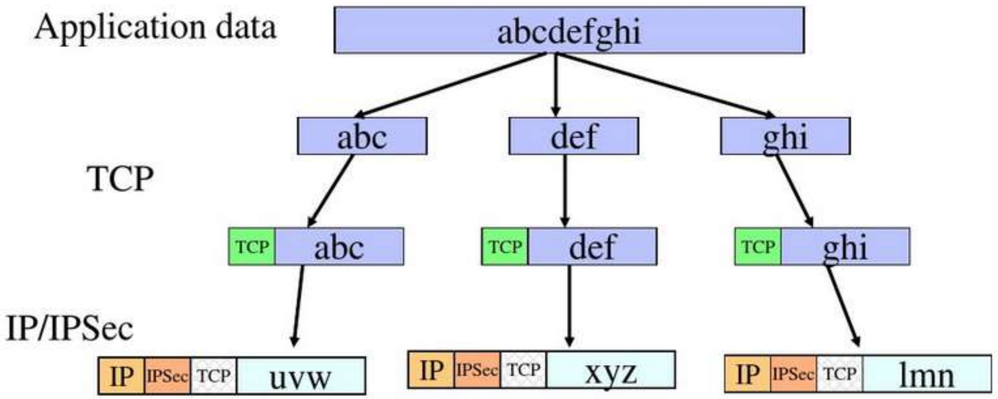
- Secure
  - Remote access
  - Intranet and extranet connectivity for external network users
  - Commercial transactions
- Any two system with compatible versions of IPSec can communicate securely over network
  - Computer and server
  - Server and firewall
  - Firewall and router…
- Two communicating systems must have the same method for exchanging encryption keys.
- The fundamental principle is:
  - Encrypt and/or authenticate all traffic on the IP layer

Data with IPSec

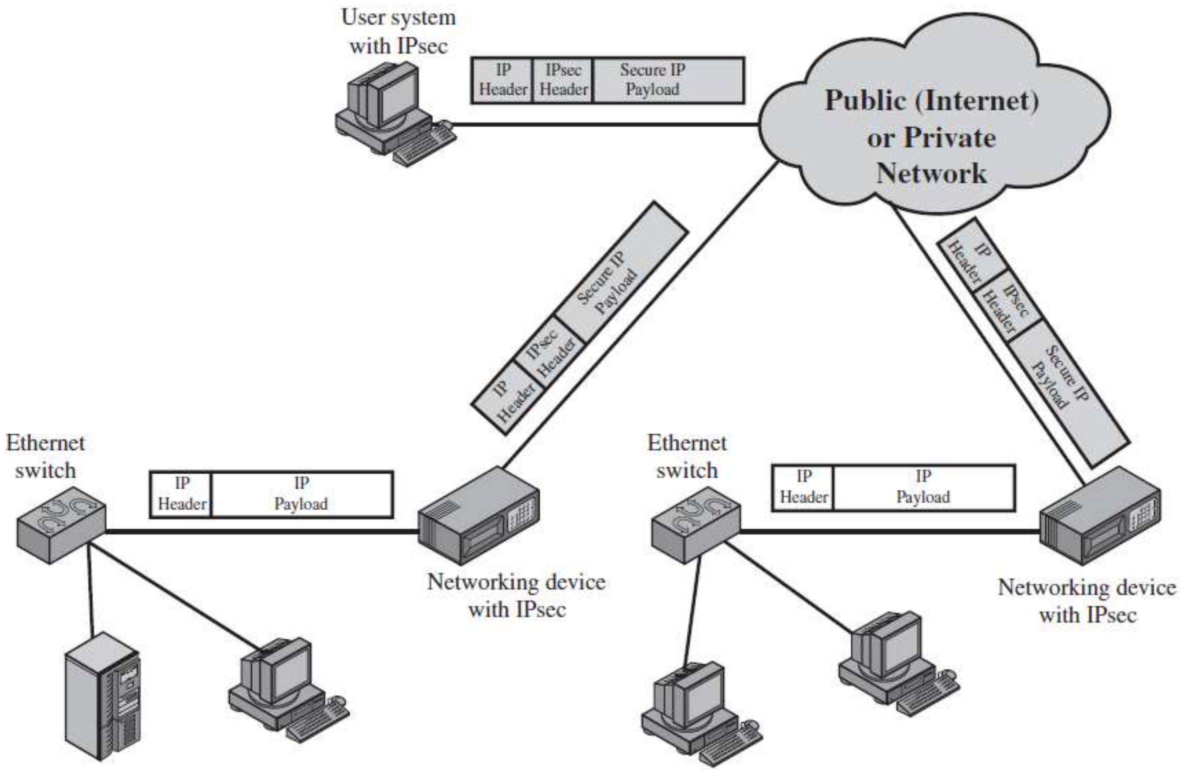
Data in TCP/IP



Data in TCP/IPSec/IP



An IP Security Scenario



IPSec Pros/Cons

- Pros:
  - Implementation in a firewall/router
    - provides strong security
    - no overhead with security related processing within an organization
  - It is below the transport layer, so it is transparent to applications and users.
  - Individualized or customized security
- Cons:
  - Is the network layer the right choice to implement security?

Stockholm University

IPSec Security Constructs

- Security Associations (SAs) and
  Security Association Database (SAD)
- Security Parameter Index (SPI)
- Security Policies and Security Policy Database (SPD)
- Selectors

Security Associations -1

- An association is a one-way relationship between a sender and a receiver that affords security services to the traffic it carries.
  - Peer situation (two-way secure exchange) requires two associations.
- Set of security information
  - Describes a particular kind of secure connection between one device and another (“a contract”)
- A device’s security association is stored in its security association database (SAD)

Security Associations -2

- Each SA is uniquely identified by a set of 3 parameters
  - Security Parameter Index (SPI): a bit string assigned to identify a SA.
    - to enable the receiving system to select a SA for the processing of the packet.
    - carried in AH and ESP headers
    - has only local significance
    - with SPI, packet flows with the same source and destination can have multiple SAs
  - IP destination address: address of a device for which SA is established. Only unicast addresses allowed; it may be an end system or a router/firewall.
  - Security protocol identifier: indicates whether the SA is for AH or ESP type.
- In any IP packet, the SA is uniquely identified by the destination address in the IP header
  - SPI in the extension header (AH and ESP)

Security Association Database (SAD)

- SADs define the parameters associated with each SA.
- The specification of authentication and privacy is independent of the key management mechanisms.
- The way in which SAD is provided is up to the implementer.
- Each SAD entry has several parameters
  - SPI: outbound and inbound
    - Outbound: used to construct the AH or ESP header
    - Inbound: map the traffic to the appropriate SA
  - Others

Parameters in an SAD Entry

Security Parameter Index	• 32-bit value selected by the receiving end of an SA to uniquely identify the SA
Sequence number counter	• 32- bit that generates the sequence number field in AH/ESP headers
Sequence counter overflow	• A flag indicating the overflow of the sequence counter - audible event and halt to the packet transmission
Anti replay window	• used to determine (the mechanism is sliding window) whether or not AH or ESP packet is a replay.
AH information	• Mechanisms and tools used by AH authentication algorithm and keys.
ESP information	• ESP authentication algorithm and keys, ESP encryption algorithms and keys, initialization vector (IV), IV mode.
Lifetime of the SA	• either a time interval or byte count after which an SA should be replaced with a new security association and (SPI) or terminated the action is clearly defined.
IPSec protocol mode	• Tunnel or transport, or wildcard
Path MTU	• an observed path maximum transmission unit and aging variables

Security Policy Database

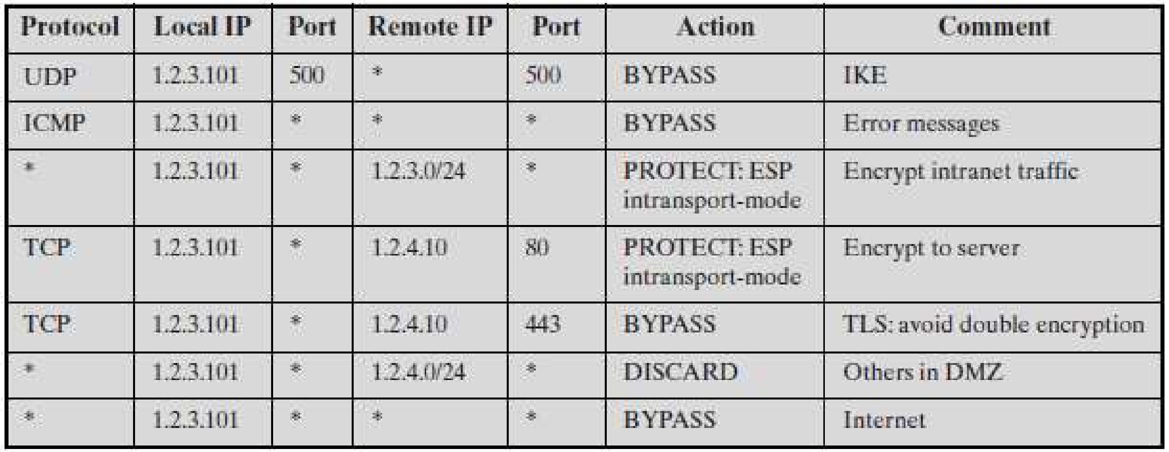
- How does a device determine which SAs to use for a specific datagram?
- The relation to or not to a SA is defined in the Security Policy Database (SPD)
  - Security Policy
    - Rules that define how to process different datagrams received by a device (from the higher layer)
    - Decide if a particular datagram needs to be processed by IPSec or not
  - Security policies for a device stored in the device’s security policy database (SPD)
- A simple case: each entry of SPD defines a subset of IP datagrams and an SA for those packets

Security Association Selectors -1

- Used to filter outgoing packet in order to map it into a particular SA.
- Defined by a set of IP and upper-layer protocol field values
  - Destination IP address : single, range or a wildcard
  - Source IP address: single, range, or a wildcard
  - User ID: a policy tied to a user or system
  - Data sensitivity level: classification of the security category
  - Transport layer protocol: an individual protocol number, a list or a range –extracted from IPv4 or IPv6 Next Header field
  - IPSec protocol: extracted from IPv4 or IPv6 NH with three possibilities –AH, ESP, or AH/ESP
  - Source or destination ports: TCP/UDP

Security Association Selectors -2

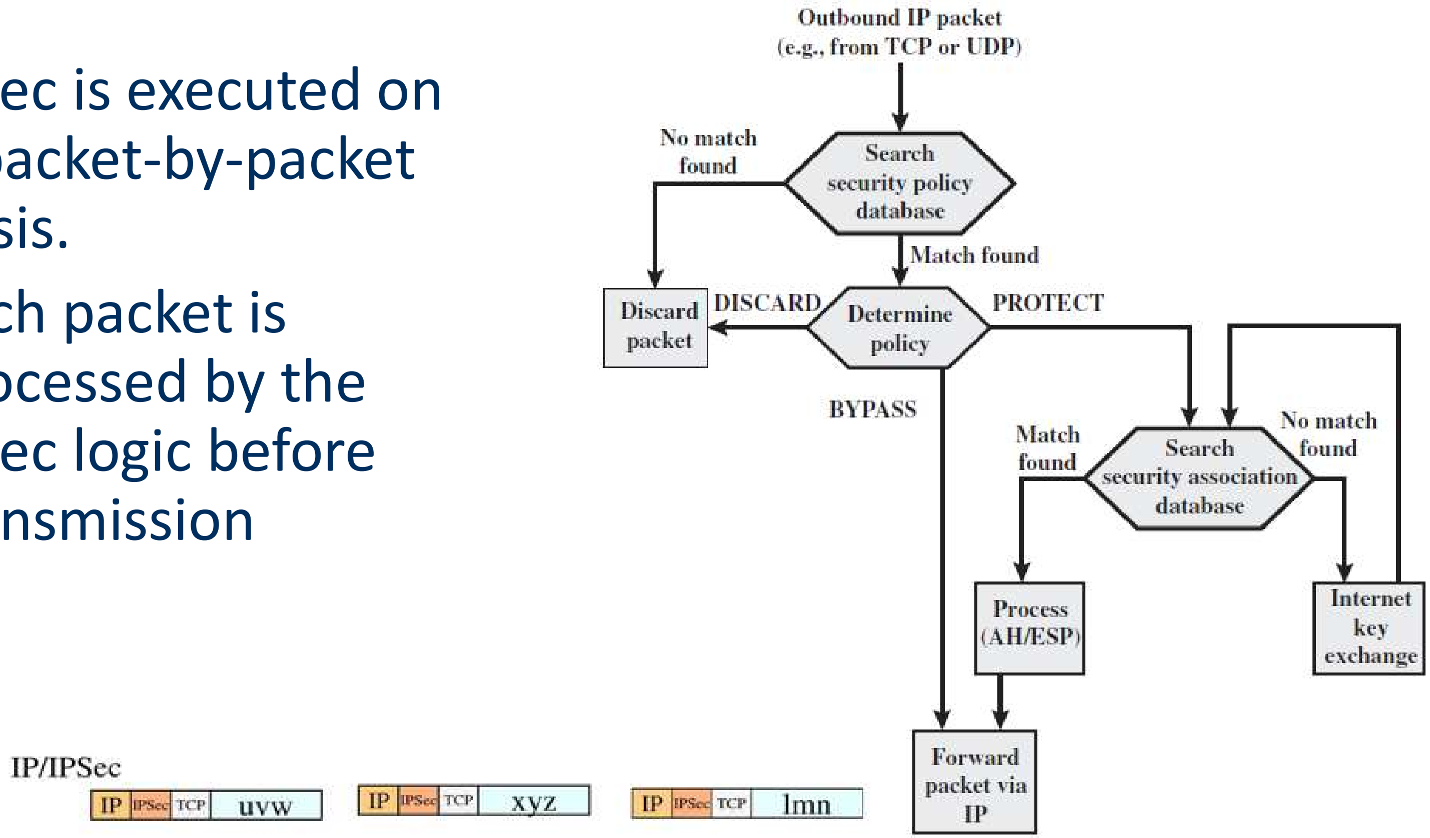
- Compare the values of the appropriate fields in the packet (the selector fields) against the SPD to find a matching SPD entry, which will point to zero or more SAs.
- Determine the SA if any for this packet and its associated SPI.



Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

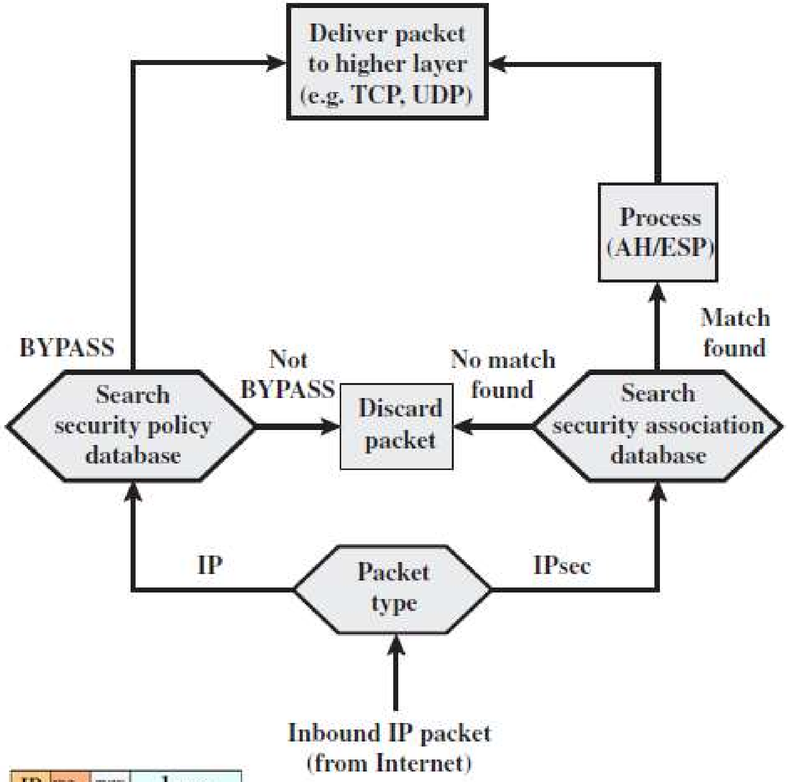
Processing Model for Outbound Packets

- IPsec is executed on a packet-by-packet basis.
- Each packet is processed by the IPsec logic before transmission



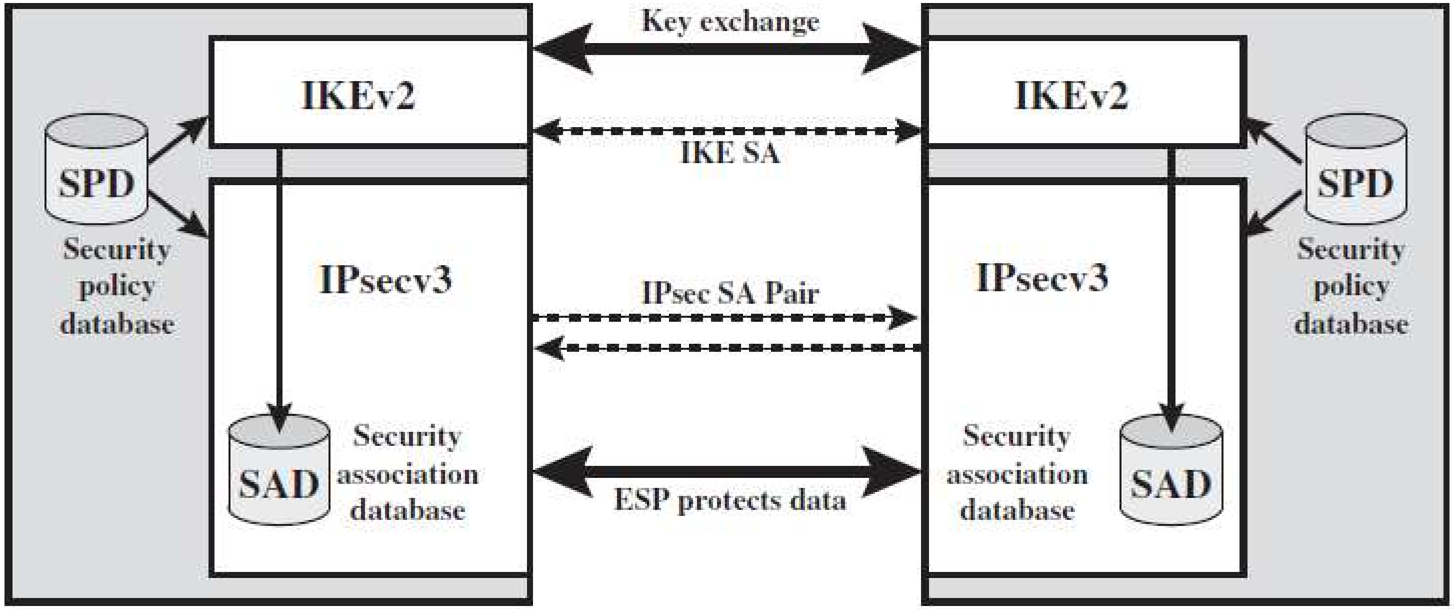
Processing Model for Inbound Packets

- An incoming IP packet triggers the IPsec processing
- Each inbound packet is processed by the IPsec logic after reception and before passing the contents on to the next higher layer (e.g., TCP or UDP).


Deliver packet to higher layer (e.g. TCP, UDP)
Process (AH/ESP)
Match found
BYPASS
Not BYPASS
No match found
Search security policy database
Discard packet
Search security association database
IP
IPsec
Packet type
Inbound IP packet (from Internet)

IP/IPSec
IP
IPSec
TCP
uvw
IP
IPSec
TCP
xyz
IP
IPSec
TCP
lmn

IPSec Architecture

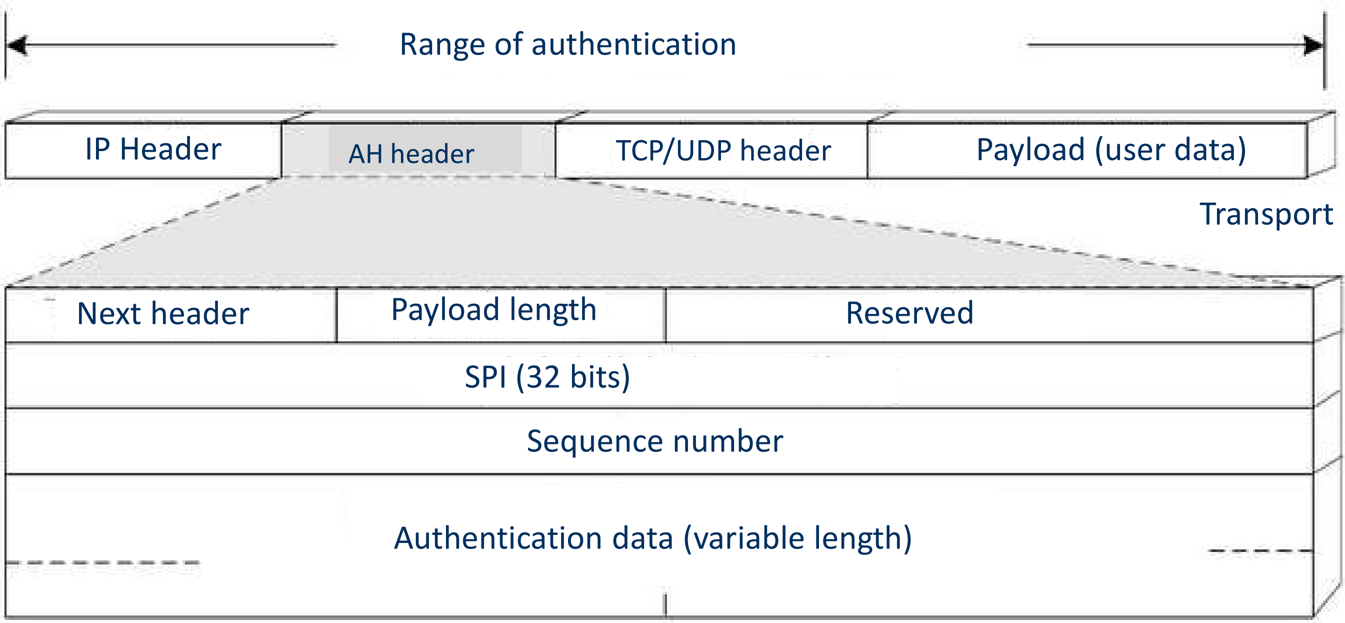


Authentication Header (AH) and Encapsulating Security Payload (ESP)

Authentication Header(AH) -1

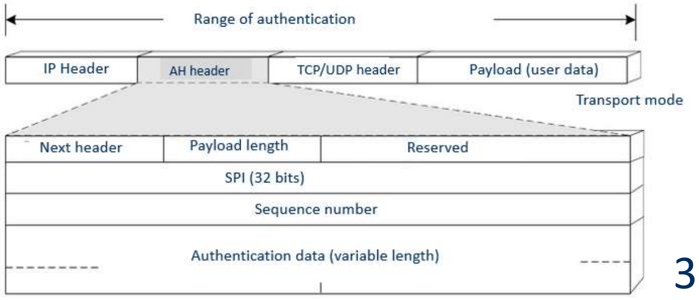
- A protocol supported by IPSec
- Provides data integrity and authentication of IP packets
  - Data integrity –no unauthorized modification of data is possible during the transmission of a packet
    - Try to protect the whole packet, except the fields that will change during the transmission, such as TTL
  - Authentication –enables network device or end system to authenticate either a user or an application, and prevent address spoofing
  - Using MAC (Message Authentication Code) to authenticate IP packets
- Provides anti-replay protection (optional)
- Does not provide confidentiality

Authentication Header (AH) -2

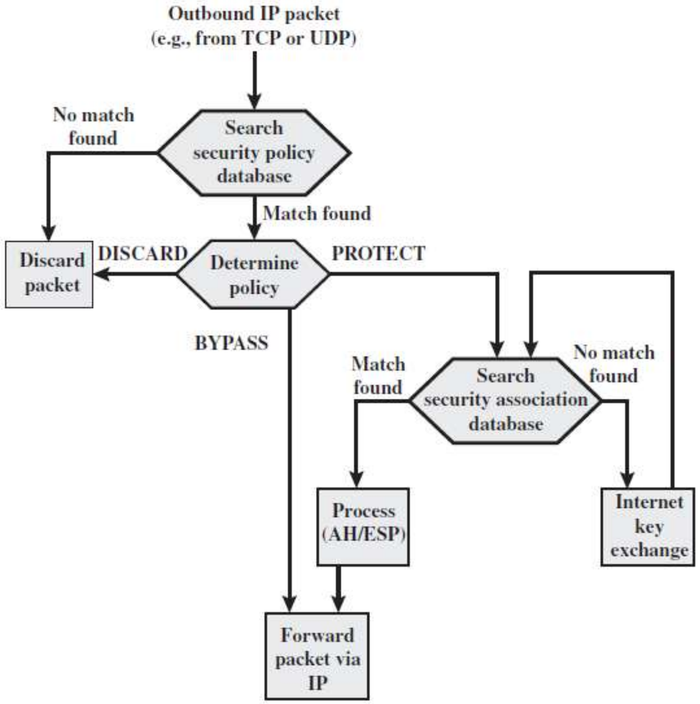


Authentication Header(AH) -2

- Security Parameters Index (SPI)
  - 32 bit reference number, agreed on by both sides of communication
  - Refers to a specific agreement between two machines to use
    - Particular encryption algorithms
    - Encryption keys, etc.
- Sequence number (32 bits)
  - Unique number
  - Applied to each packet in the IPSec session, to prevent replay attack
- Authentication Data includes information used to verify integrity
  - Integrity Check Value (ICV)
    - Message Authentication Code (MAC)
    - Hash function (SHA)

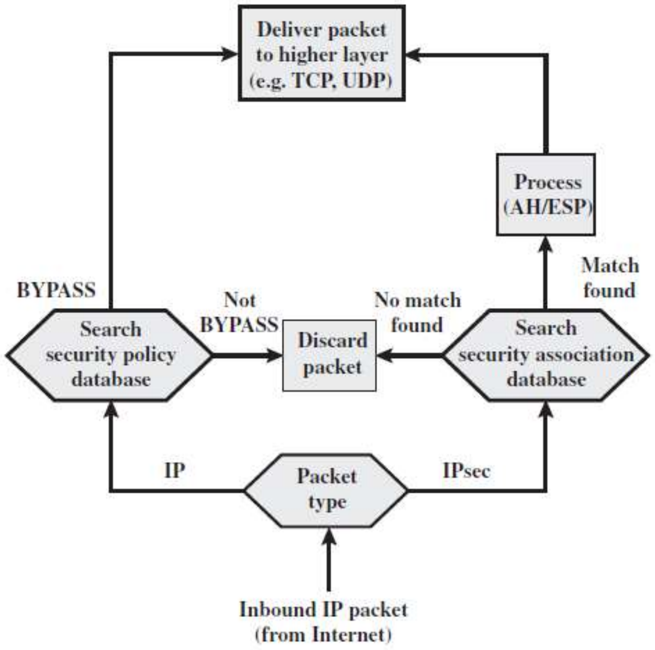


AH Processing for Outbound Packets



- AH Process
  - Create or increase the sequence number
  - Calculate ICV
  - Forward the packet

AH Processing for Inbound Packets


Deliver packet to higher layer (e.g. TCP, UDP)
Process (AH/ESP)
BYPASS
Match found
Not BYPASS
No match found
Search security policy database
Discard packet
Search security association database
IP
Packet type
IPsec
Inbound IP packet (from Internet)

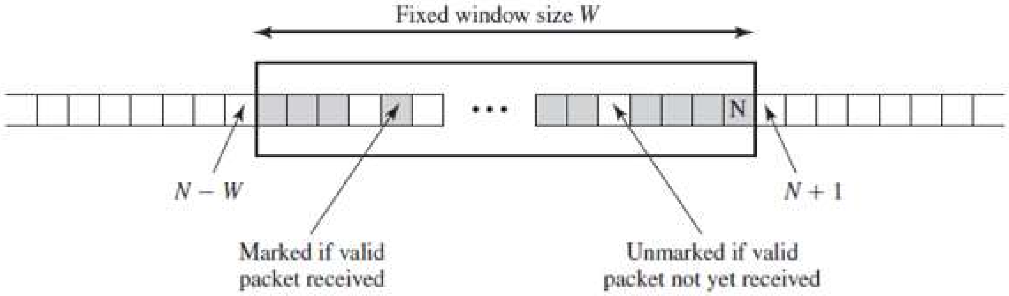
- AH Process
- Check sequence number to see if it is re-play
- Calculate ICV according to the algorithms specified in SA, and compare it with the ICV in the authentication data field
  - if the two values are different, then discard the packet
- AH support HMAC-MD5 and HMAC-SHA1

Anti-replay -1

- Replay: a copy of the original data is captured and later replayed by the attacker to a specific destination.
- Replay attack: which an attacker obtains a copy of an **authenticated packet** and later transmits it to the intended destination.
- Defense: Sequence Number field
  - When a new SA is established, a 32-bit sequence number counter is initialized to zero
  - The sender increases the counter after each packet is sent on this SA, e.g., the first packet uses sequence number 1.
  - When the anti-replay is enabled (default) the transmitted sequence number cannot be repeated/cycled
  - When the counter limit is reached the current SA should be terminated and a new one negotiated

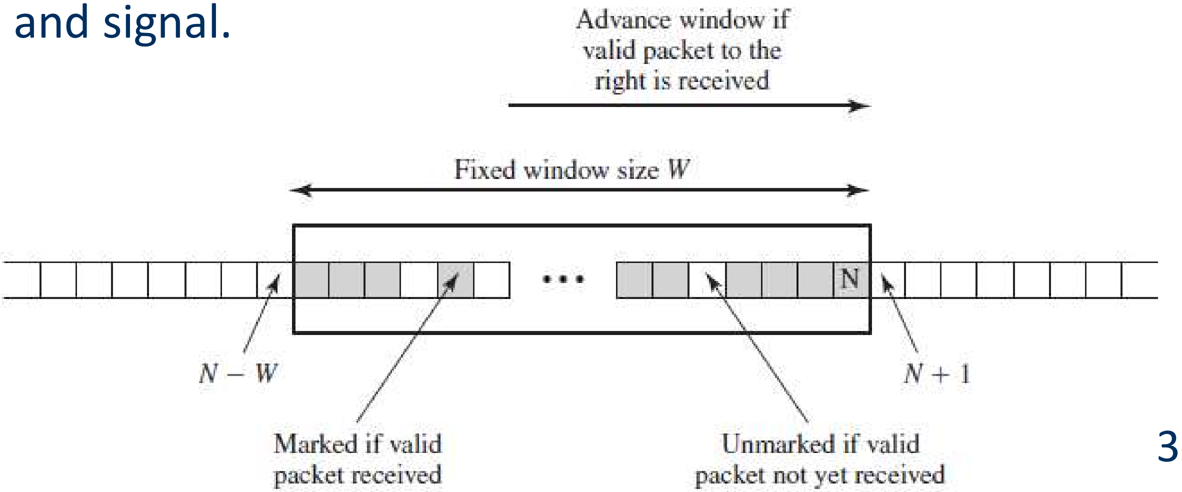
Anti-replay -2

- IP uses a Best-Effort service model (no guarantees for complete and in order delivery)
- IPSec requests that the receiver implements a receiving window with size W (default is 64)
  - The right edge of the window represents the highest sequence number N so far received for a valid packet.
  - For any packet with a sequence number in the range of (N-W+1 to N) that is properly received (authenticated), the corresponding slot in the window is marked.


Fixed window size W
N
• • •
$N - W$
$N + 1$
Marked if valid packet received
Unmarked if valid packet not yet received

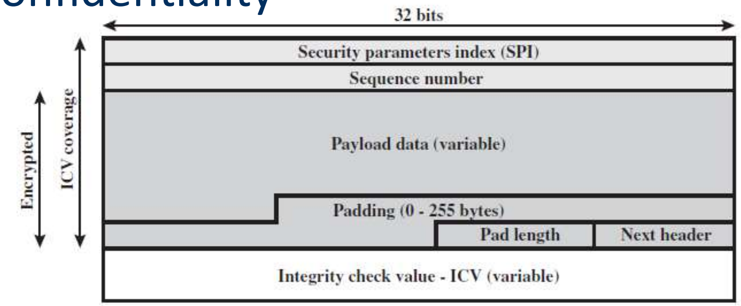
Anti-replay –Sliding Window

1. If the packet is within the window size and is a new packet, then check the MAC. If the authentication is OK then the corresponding slot is marked.
2. If the packet is to the right of the window and is a new packet, then check the MAC. If authentication is OK, then increase the size of the window W , and mark the slot.
3. If the packet is to the left of the window, and authentication is not OK, discard the packet and signal.


Advance window if valid packet to the right is received
Fixed window size W
N
•••
$N - W$
$N + 1$
Marked if valid packet received
Unmarked if valid packet not yet received

Encapsulating Security Payload (ESP)

- Provides data confidentiality, data origin authentication, connectionless integrity, anti-replay, limited traffic flow confidentiality
- ESP encrypts the following fields:
  - Payload Data
  - Padding
  - Padding Length
  - Next Header



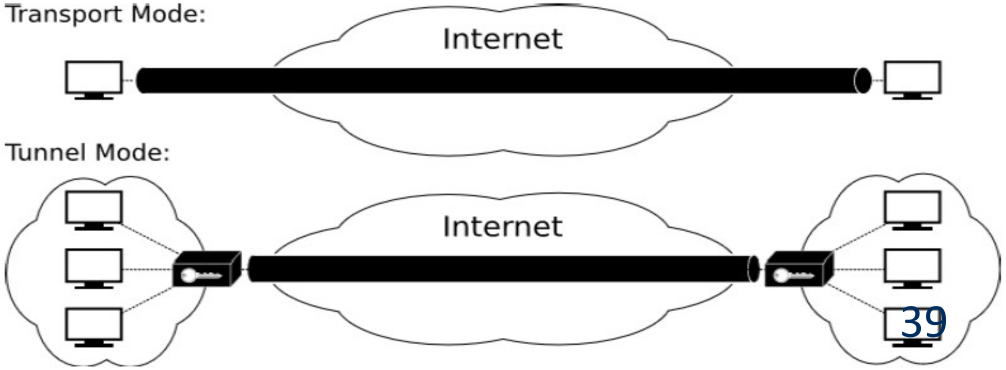
(a) Top-level format of an ESP Packet

- In most cases ESP uses symmetric encryption: for simplicity reasons
- ESP can work with a variety of encryption and authentication algorithms
- If the encryption algorithm requires cryptographic synchronization data such as an Initialization Vector (IV), it may be carried out explicitly at the beginning of the Payload Data field.

IPSec Operation Mode

Modes of Operation

- IPSec defines two specific modes of operation that are related to the IPSec architecture
  - Transport mode
    - Authentication is provided directly between two parties (e.g., a server and client)
    - Can be on the same network or external network
    - If they share a protected key the process is secure
  - Tunnel mode
    - Remote workstation authenticates itself to the firewall for access to the entire internal network



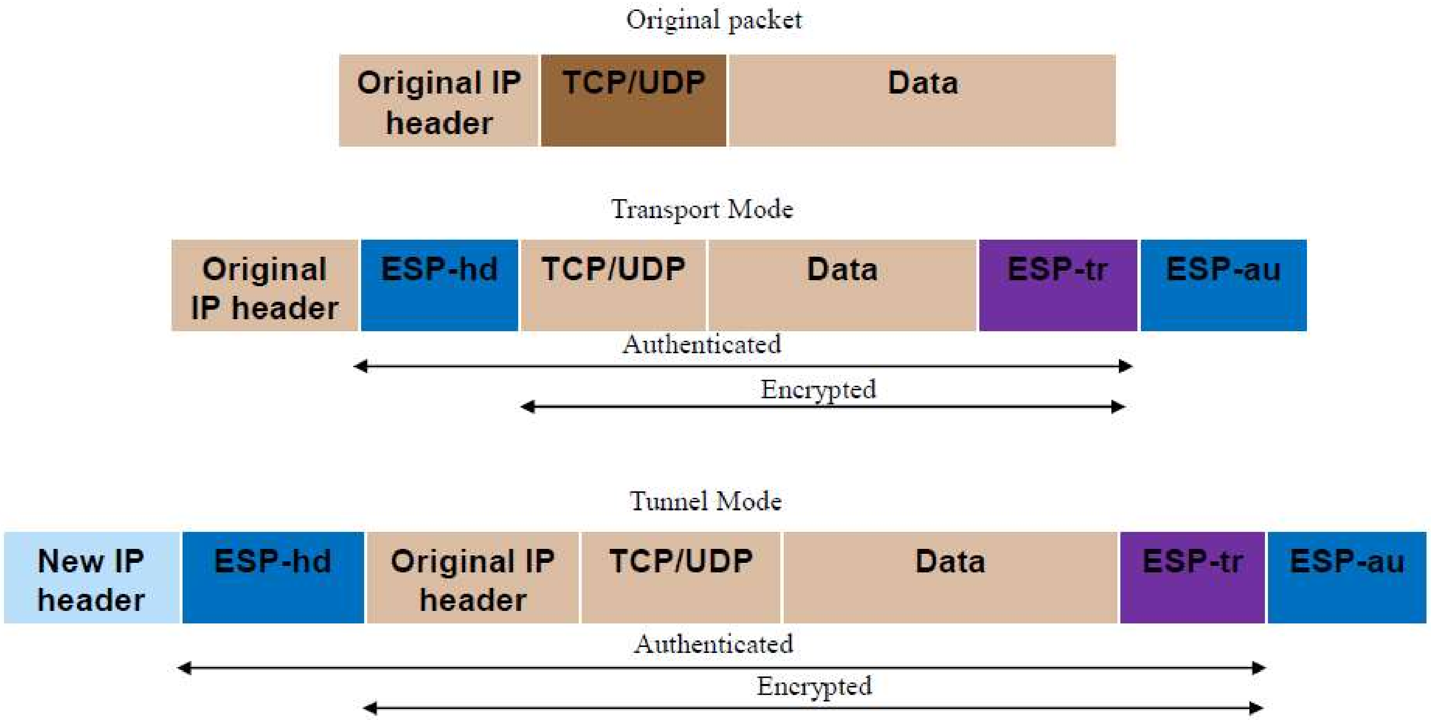
Transport Mode

- Used to protect E2E communications between two hosts (server-client, two servers)
- Protection is either authentication or encryption (or both)
  - ESP in transport mode encrypts and optionally authenticates the IP payload, but not the header.

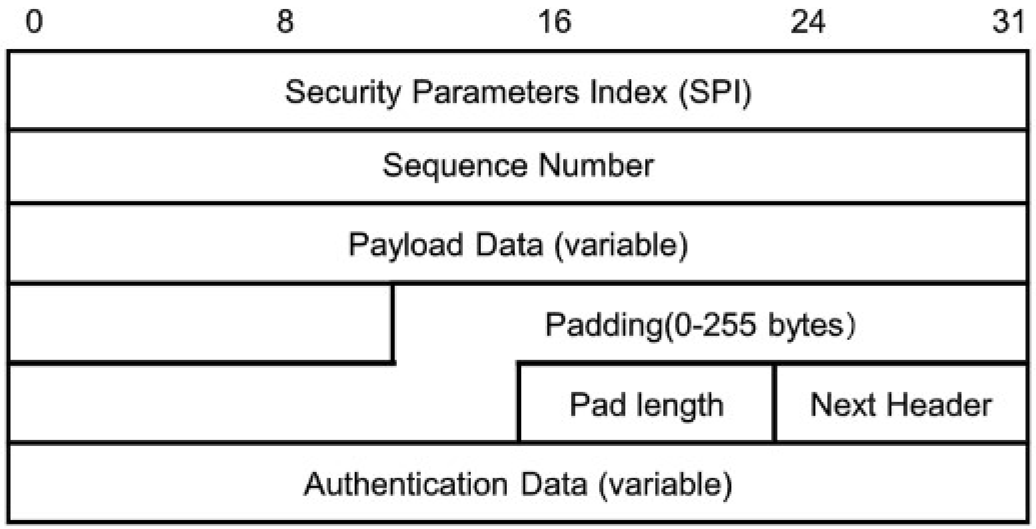
Tunnel Mode

- Encapsulates the entire IP packet within an IP packet
  - makes sure that no part of the original packet is being modified in transit
- A tunnel is built
  - The inner packet will become “invisible” for the routers along the way
- The “visible” header contains enough data to make it move through the routers, yet not sufficient for traffic analysis
- Tunnel mode is used when both ends of a connection end with a firewall or router that implements IPSec

Scope of ESP in IPv4 (Authentication and Encryption)



ESP Header and Trailer



0 8 16 24 31

Security Parameters Index (SPI)

Sequence Number

Payload Data (variable)

Padding(0-255 bytes)

Pad length

Next Header

Authentication Data (variable)

Key Management

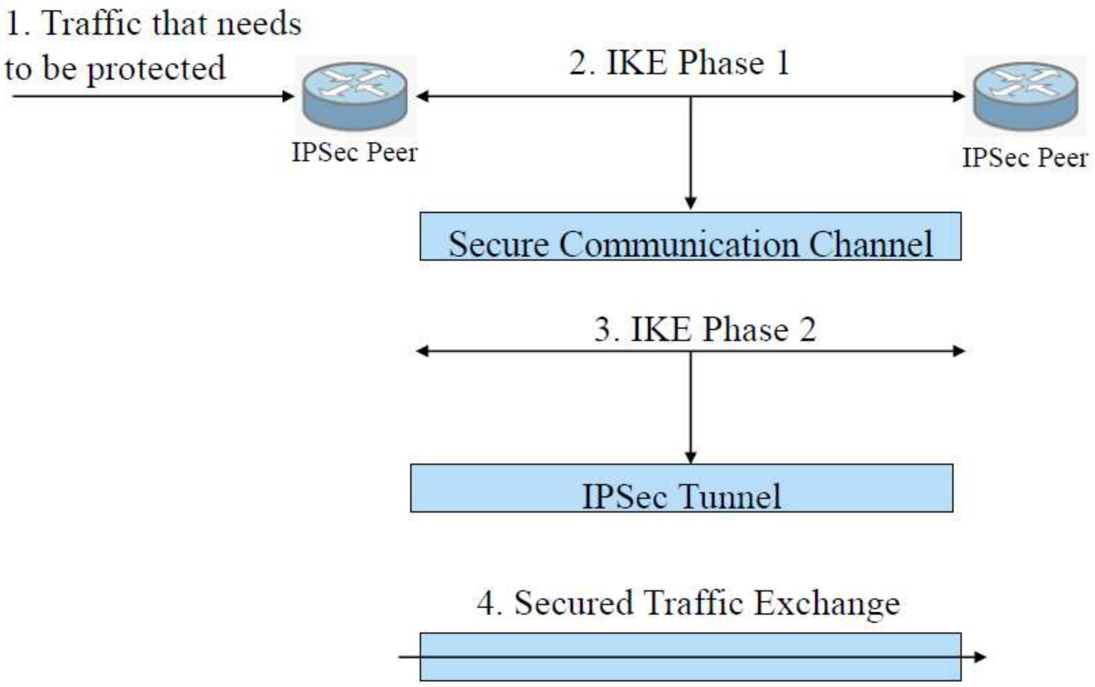
Key Management

- Key Management in IPSec involves
  - Determination and distribution of secret keys
  - Negotiates the Security Association for IPSec
- Two ways
  - Manually: appropriate for small and static environments
  - Automated: creating keys for SA on demand.
    - Facilitates the use of keys in large distributed networks.
    - Requires more effort and knowledge.
- The default automated key management protocol of IPSec is Internet Key Exchange (IKE).

Internet Key Exchange (IKE)

- Internet Security Association and Key Management Protocol (ISAKMP)
  - Provides a framework for Internet key management and specific protocol support, including formats, for negotiation of security attributes.
  - Used for establishing SA and cryptographic keys
- IKEv2
  - Creates a secure tunnel between two entities
  - Negotiates the Security Association for IPSec
  - Provides generation of shared keys
  - Key exchange based on Diffie-Hellman algorithm + additional security
  - Uses UDP port 500

IKE Working Procedure - Two phases, Four steps


1. Traffic that needs to be protected
IPSec Peer
2. IKE Phase 1
IPSec Peer
Secure Communication Channel
3. IKE Phase 2
IPSec Tunnel
4. Secured Traffic Exchange

1. Traffic that is identified to require IPSec protection to its destination is generated or received by one of the IPSec peers
2. IKE phase 1 establishes a secure authenticated channel IKE SA between two peers (involves negotiating IKE policy, performing authenticated DH exchange, protecting IKE peers identity)
3. Phase 2 results in the creation of two IPSec SAs between the two IPSec peers (secure IPSec tunnel)
4. Data is transmitted between the IPSec peers over the established secure IPSec tunnel

Summary

- IPSec is a capability that can be added to IPv4 or IPv6 by using extended headers.
- IPSec involves three aspects: authentication, confidentiality, key management.
- IPSec works at Layer 3 of OSI reference model
  - Authenticate/encrypt each packet
  - Secure applications/protocols from the higher layers

- Big overhead

Expected Learning Outcomes

- Understand and explain the principles of IPSec (including AH and ESP)
- Understand and explain how AH and ESP can be used
- Understand and describe the key exchange method of IPSec
- Understand and explain the advantages and disadvantages of IPSec

Thank you!