Chapter 19

IP Security

IP Security

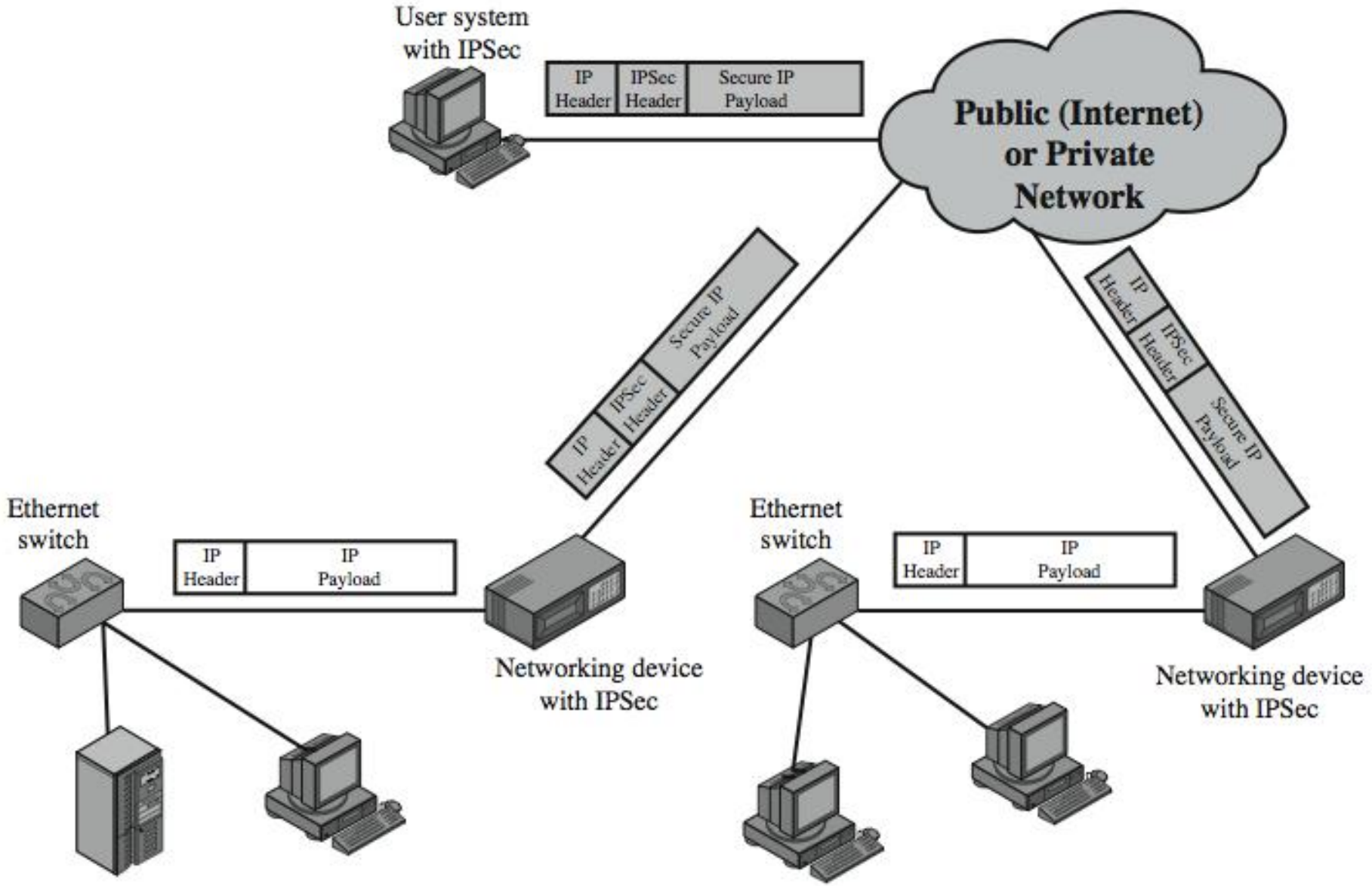
- Internet has a range of security mechanisms in applications.
  - E.g. electronic mail [S/MIME, PGP], client/server [Kerberos], Web access [SSL/HTTPS], and others.
- There are security concerns that cut across protocol layers
- Security implemented by the network for all applications

IP Security

- IP-Security provides
  - **Authentication:** Assures that a received packet was transmitted by the party identified as the source in the packet header, and that the packet has not been altered in transit.
  - **Confidentiality:** Enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
  - **Key management:** Concerned with the secure exchange of keys.

- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.

IP Security Uses



IP Security Uses

- An organization maintains LANs at dispersed locations.
- Unsecure IP traffic is conducted on each LAN and IPSec protocols are used for outside traffic through WAN.
- IPSec operates in networking devices such as a router or firewall that connect each LAN to the outside world.
- The IPSec networking device will typically encrypt and compress all traffic going into the WAN, and decrypt and decompress traffic coming from the WAN.
- Secure transmission is also possible with individual users who dial into the WAN. Such user workstations must implement the IPSec protocols to provide security.

Benefits of IPSec

- In a firewall/router provides strong security to all traffic crossing the perimeter
- In a firewall/router is resistant to bypass
- Is below transport layer (TCP, UDP), hence transparent to applications
  - If IPsec is implemented in end systems, upper-layer software, including applications, is not affected.
- Can be transparent to end users
- Can provide security for individual users
  - This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.
- secures routing architecture

IP Security Architecture

- IPSec specification is quite complex, with groups:
  - **Architecture:** Covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology
    - RFC4301 *Security Architecture for Internet Protocol*
  - **Authentication Header (AH):** An extension header for message authentication
    - RFC4302 *IP Authentication Header*
  - **Encapsulating Security Payload (ESP):** Consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication.
    - RFC4303 *IP Encapsulating Security Payload (ESP)*
  - **Internet Key Exchange (IKE):** A collection of documents describing the key management schemes for use with IPsec
    - RFC4306*Internet Key Exchange (IKEv2) Protocol*
  - **Cryptographic algorithms:** A large set of documents that define and describe cryptographic algorithms for encryption, message authentication, pseudorandom functions (PRFs), and cryptographic key exchange.
  - **Other**

IPSec Services

- IPSec provides security services at the IP layer by enabling a system to :
  - Select required security protocols.
  - Determine the algorithm(s) to use for the service(s).
  - Put in place any cryptographic keys required to provide the requested services.
- Two protocols are used to provide security:
  - An authentication protocol designated by the header of the protocol, Authentication Header (AH).
  - A combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP).

IPSec Services

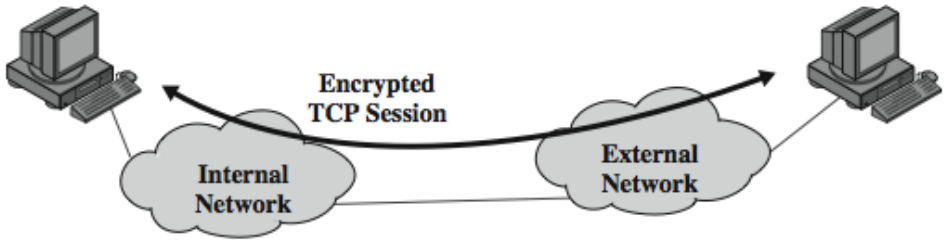
- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - A form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality

Transport and Tunnel Modes

- Transport Mode
  - to encrypt & optionally authenticate IP data
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic.
  - provides confidentiality for any application that uses it.
- Tunnel Mode
  - encrypts entire IP packet
  - add new header for next hop
  - no routers on way can examine inner IP header
  - good for Virtual Private Networks (VPNs), gateway to gateway security

Transport and Tunnel Modes

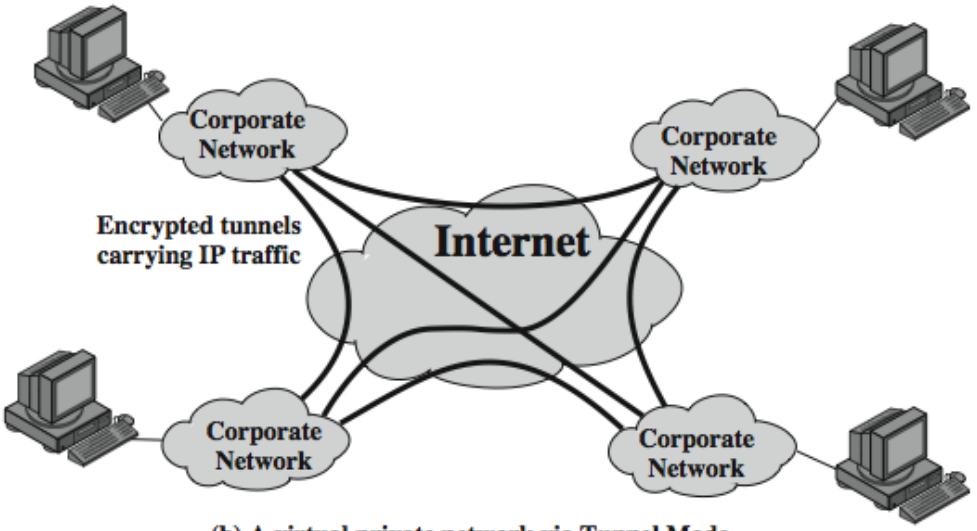
Encryption (and optionally authentication) is provided directly between two hosts.



(a) Transport-level security

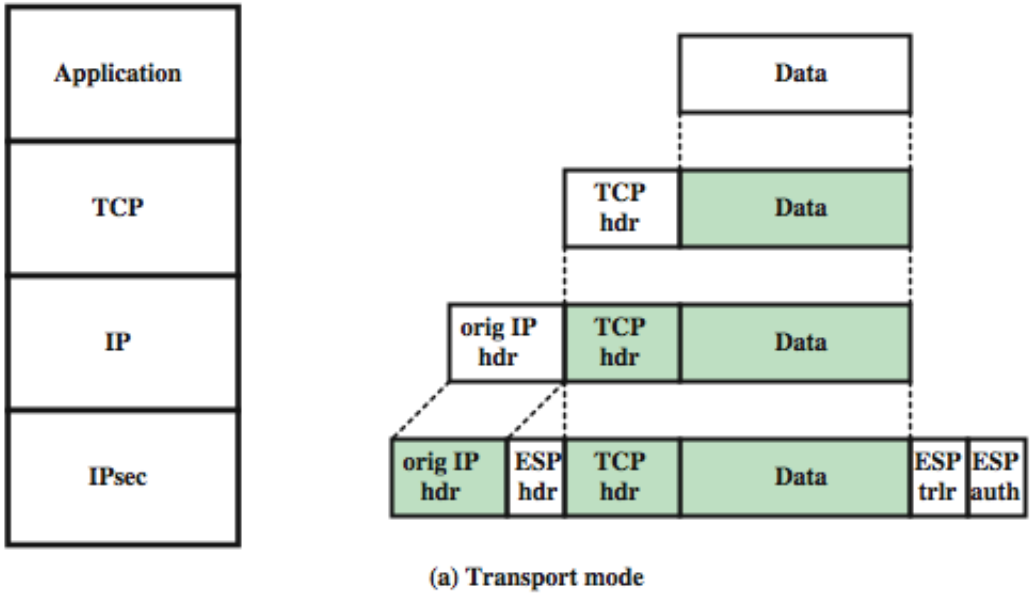
How tunnel mode operation can be used to set up a **virtual private network**.

Ex., An organization has four private networks interconnected across the Internet. Hosts on the internal networks use the Internet for transport of data but do not interact with other Internet- based hosts.

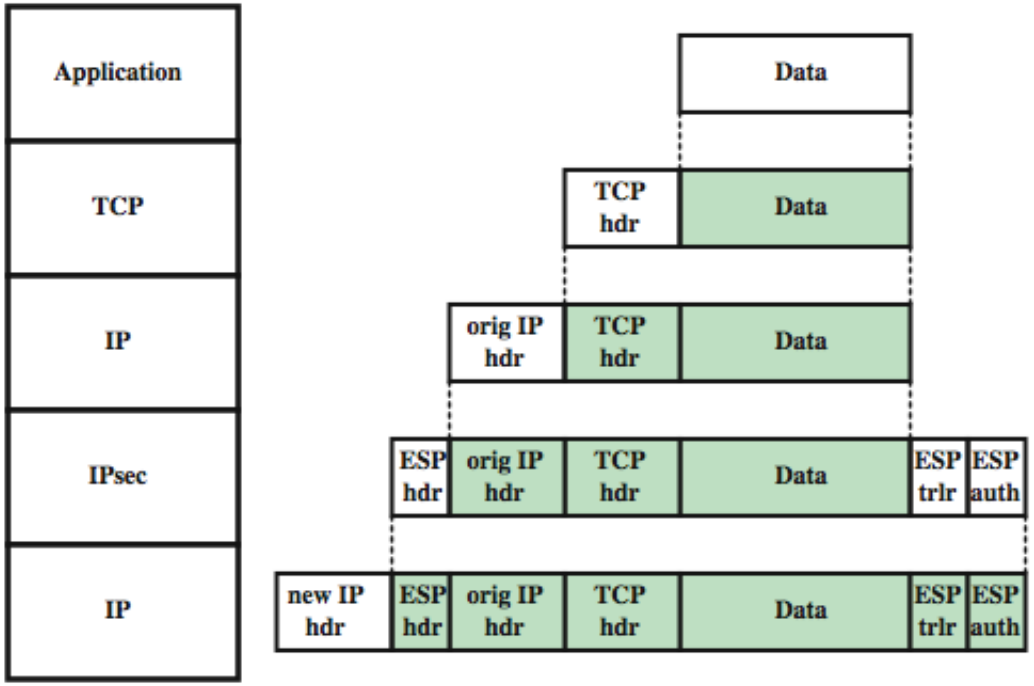


(b) A virtual private network via Tunnel Mode

Transport and Tunnel Mode Protocols



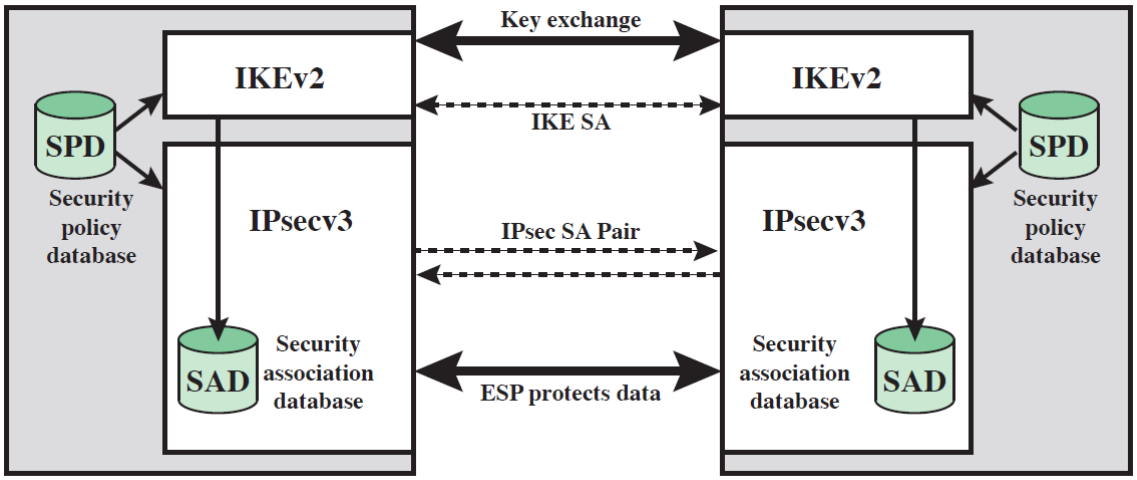
(a) Transport mode



(b) Tunnel mode

IP Security Policy

- Policy applied to each IP packet that transits from a source to a destination.
- Determined by the interaction of two databases
  - Security Association Database (SAD)
  - Security Policy Database (SPD)



IPsec Architecture

Security Associations

- **Security Association (SA) :** A key concept that appears in both the authentication and confidentiality mechanisms for IP.
  - SA is a one-way relationship between sender & receiver that affords security for traffic flow
  - If a peer relationship is needed for two-way secure exchange, then two SA are required.
  - Security services are afforded to an SA for the use of AH or ESP, but not both.

- ***SA Defined by 3 parameters:***
  - **Security Parameters Index (SPI):** Carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
  - **IP Destination Address:** The address of the destination endpoint of the SA
  - **Security Protocol Identifier:** Indicates whether the association is an AH or ESP security association.

- **SA has a number of other parameters**
  - seq no, AH & ESP info, lifetime … etc

- **There is a SA Database that defines the parameters associated with each SA.**
  - Security Association Database (SAD)

Security Policy Database (SPD)

- Relates IP traffic to specific Security Associations (SAs)
  - Match subset of IP traffic to relevant SA
  - Use selectors to filter outgoing traffic to map it to particular SA
  - Selector based on: local & remote IP addresses, next layer protocol, name, local & remote ports

Processing of Outbound Packets

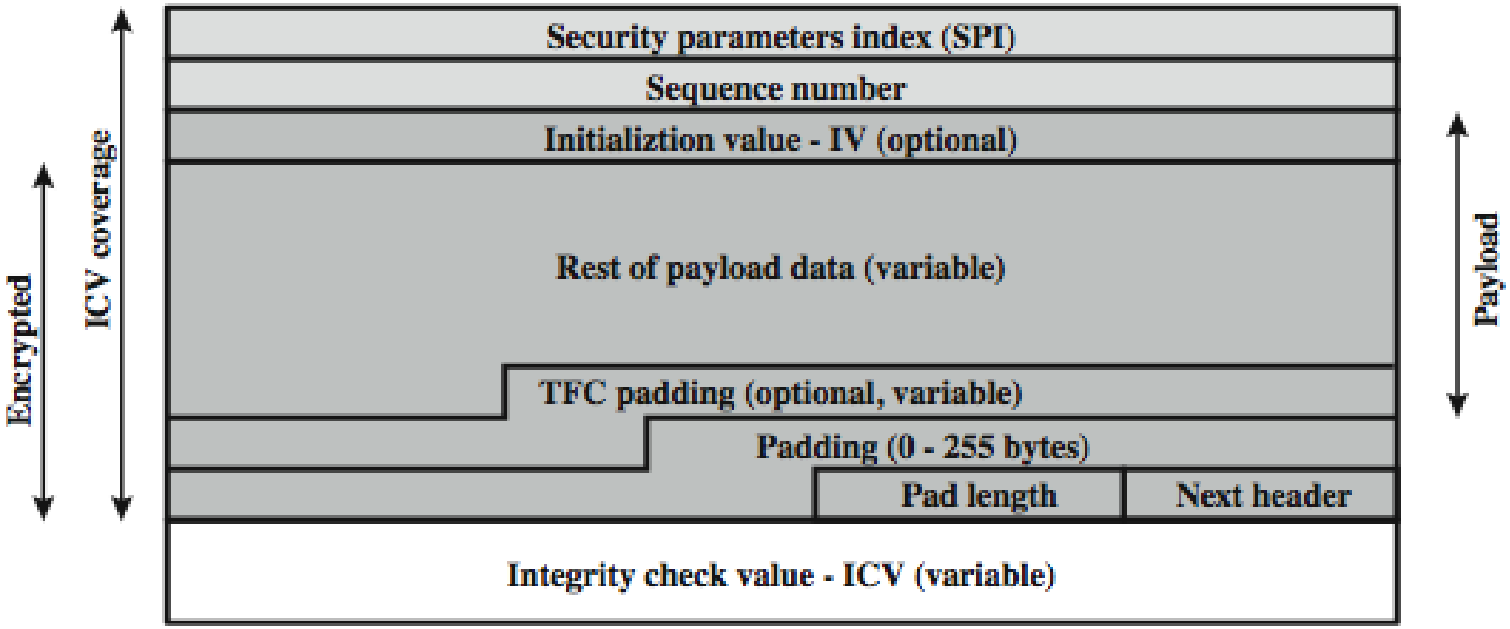
- **Outbound processing obeys the following general sequence for each IP packet.**

1. 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.
2. Determine the SA if any for this packet and its associated SPI.
3. Do the required IPSec processing (i.e., AH or ESP processing).

Encapsulating Security Payload (ESP)

- Provides message content confidentiality, data origin authentication, connectionless integrity, an anti-replay service, limited traffic flow confidentiality
- Provided services depend on options selected when establish Security Association (SA).
- Can use a variety of encryption & authentication algorithms

Encapsulating Security Payload



- **Security Parameters Index (32 bits):** Identifies a security association
- **Sequence Number (32 bits):** An increasing counter value; this provides an anti-replay function
- **Payload Data (variable):** A transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption
- **Padding (0–255 bytes):** for various reasons
- **Pad Length (8 bits):** the number of pad bytes immediately preceding this field
- **Next Header (8 bits):** identifies the type of data in the payload data field
- **Integrity check value (variable):** A variable-length field contains the Integrity Check Value computed over the ESP packet

Two additional fields may be present in the payload.

An initialization value (IV), or nonce, present if this is required by the encryption or authenticated encryption algorithm used for ESP. If tunnel mode is being used, then the IPsec implementation may add **Traffic Flow Confidentiality (TFC)** padding after the Payload Data and before the Padding field.

Encryption & Authentication Algorithms & Padding

- ESP can encrypt payload data, padding, pad length, and next header fields
  - if needed have IV at start of payload data
- ESP can have optional ICV for integrity
  - is computed after encryption is performed
- ESP uses padding
  - to expand plaintext to required length
  - to align pad length and next header fields
  - to provide partial traffic flow confidentiality

Anti-Replay Service

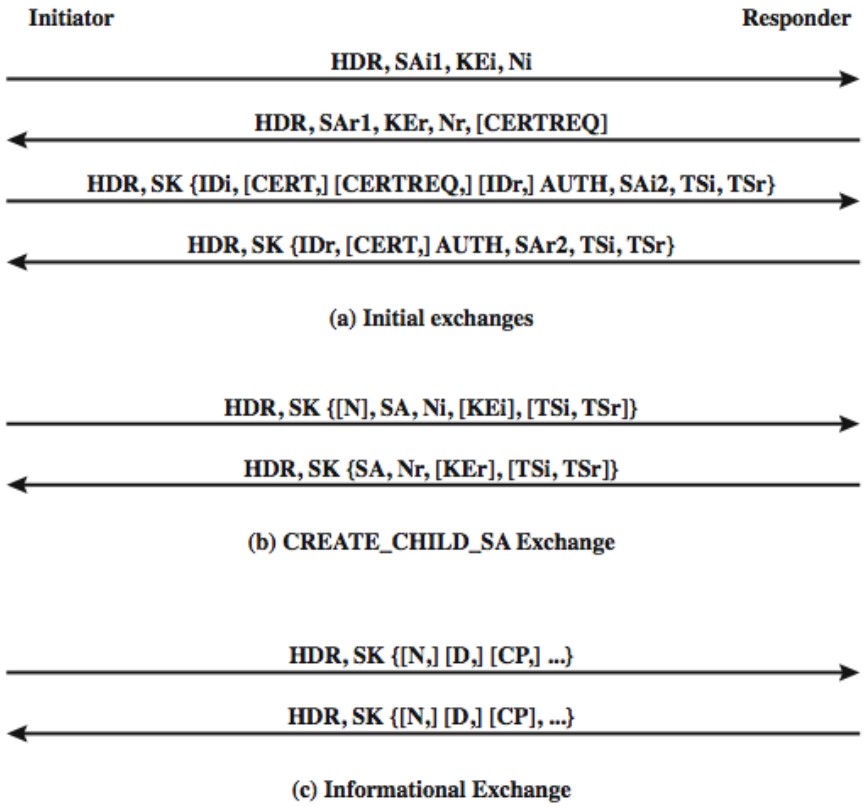
- Replay is when attacker resends a copy of an authenticated packet
- Use sequence number to thwart this attack
- Sender initializes sequence number to 0 when a new SA is established
  - increment for each packet
  - must not exceed limit of $2^{32} - 1$
  - If the limit of $2^{32}-1$ is reached, the sender should terminate this SA and negotiate a new SA with a new key.
- receiver then accepts packets with seq. no within window of

  ($N - W+1$) to N
  - Where W is a window size (W packets)

IPSec Key Management

- Handles key generation & distribution
- Typically need 2 pairs of keys
  - 2 per direction [transmit and receive] for AH & ESP
- Manual key management
  - Sysadmin manually configures every system with its own keys and with the keys of other communicating
- Automated key management
  - automated system for on demand creation of keys for SA's in large distributed systems

IKEV2 Exchanges

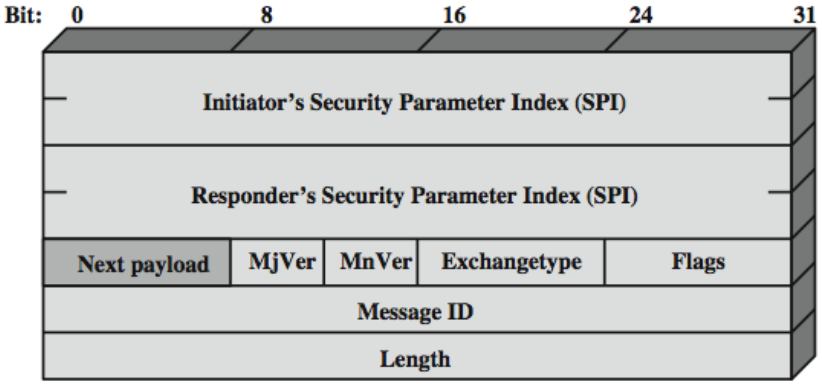


The IKEv2 protocol involves the exchange of messages in pairs

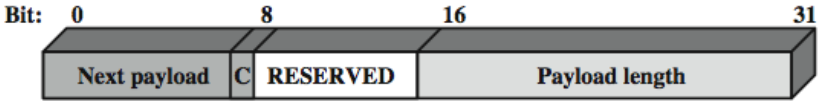
- **Initial exchanges**, exchange information concerning cryptographic algorithms and other parameters they are willing to use along with nonces and Diffie-Hellman (DH) values. The result of this exchange is to set up a special SA called [IKE SA]. All subsequent IKE message exchanges are protected by encryption and message authentication.
- **In the second exchange**, the two parties authenticate one another and set up a first IPsec SA to be placed in the SADB and used for protecting ordinary (i.e. non-IKE) communications between the peers.
  - Four messages are needed to establish the first SA for general use. The **CREATE_CHILD_SA** Exchange can be used to establish further SAs for protecting traffic.
  - **Informational exchange** is used to exchange management information, IKEv2 error messages, and other notifications.

Internet Security Association and Key Management Protocol

ISAKMP



(a) IKE Header



(b) Generic Payload Header

- **ISAKMP** message consists of ISAKMP header followed by one or more payloads, carried in a transport protocol (UDP by default).
- **The header format for an ISAKMP message includes the fields:**
  - Initiator SPI (64 bits): chosen by the initiator to identify a unique SA
  - Responder Cookie (64 bits): chosen by responder to identify unique IKE SA
  - Next Payload (8 bits): type of the first payload in the message.
  - Major/Minor Version (4 bits): Indicates major/minor version of IKE in use
  - Exchange Type (8 bits): type of exchange.
  - Flags (8 bits): specific options set for this IKE exchange.
  - Message ID (32 bits): control retransmission, matching of requests /responses.
  - Length (32 bits): of total message (header plus all payloads) in octets.
- **All ISAKMP payloads begin with the same generic payload header shown in Figure (b).**
  - The Next Payload field has a value of 0 if this is the last payload in the message; otherwise its value is the type of the next payload.
  - The Payload Length field indicates the length in octets of this payload, including the generic payload header.
  - The critical bit is zero if the sender wants the recipient to skip this payload if it does not understand the payload type code in the Next Payload field of the previous payload. It is set to one if the sender wants the recipient to reject this entire message if it does not understand the payload type.

IKE Payloads & Exchanges

- have a number of ISAKMP payload types:
  - Security Association, Key Exchange, Identification, Certificate, Certificate Request, Authentication, Nonce, Notify, Delete, Vendor ID, Traffic Selector, Encrypted, Configuration, Extensible Authentication Protocol
- Payload has complex hierarchical structure
- Contain multiple proposals, with multiple protocols & multiple transforms

Cryptographic Suites

- The IPsecv3 and IKEv3 protocols rely on a variety of cryptographic algorithm types
- to promote interoperability have
  - RFC4308 defines VPN cryptographic suites
    - VPN-A matches common corporate VPN security using 3DES & HMAC
    - VPN-B has stronger security for new VPNs implementing IPsecv3 and IKEv2 using AES
  - RFC4869 defines four cryptographic suites compatible with US NSA specs
    - provide choices for ESP & IKE
    - AES-GCM, AES-CBC, HMAC-SHA, ECP, ECDSA